Technická univerzita v Liberci
Ekonomická fakulta

Studijní program: **M 6209 –** Systémové inženýrství a informatika
Studijní obor: Manažerská informatika

Návrh webhostingového řešení

Proposal for web hosting solution

DP – EF – KIN – 2010 – 22

Jiří Semrád

Vedoucí práce: doc. Ing. Jan Skrbek, Dr., katedra informatiky
Konzultant: Ing. Michal Houšť, NG Systém

Počet stran: 74 Počet příloh: 3

Datum odevzdání: 7.května 2010

Prohlášení

Byl(a) jsem seznámen(a) s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom(a) povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracoval(a) samostatně s použitím uvedené literatury a na základě konzultací s vedoucím diplomové práce a konzultantem.

V Liberci dne 5.1.2010 ……..

Anotace

Tato práce se zabývá návrhem webhostingového řešení. V její první části se zabývám právní problematikou, která je spojena s poskytováním webového prostoru na Internetu. V této části řeším aspekty z pohledu vlastníka webhostingu a jeho postoj k právní odpovědnosti. V další části se již zabývám jednotlivými prvky webhostingu, snažím se vybrat a vysvětlit proč zrovna ten daný prvek je vhodný pro webhosting. Další významnou kapitolou vyskytující se v této práci je otázka bezpečnosti, dnes tolik diskutovaná. Prvé řadě jsem se zastavil nad problematikou fyzického zajištění serveru proti okolním vlivům. V další části již řeším softwarou stránku bezpečnosti a jak nejlépe aplikovat jednotlivé bezpečnostní prvky. Další kapitola již zahrnuje analýzu technického řešení serveru s přihlédnutím k ekonomickým aspektům. A v neposlední řadě tato práce obsahuje testování webhostingového řešení, které jsem navrhnul a zkompiloval na svém počítači.

Klíčová slova

Apache, hosting, Internet, ISPConfig, Linux, počítačová bezpečnost, server, web, webhosting

Annotation

This work deals with proposal of webhosting solution. In the first part I am solving a problem with legal issue, which is associated with the providing web space on the Internet. In this part I am looking at the aspects from the webhosting owner perspective and his attitude to legal liability. The next section is dealing with several parts of the webhosting, and I am trying to find and explain which part is the best and suitable for webhosting solution. The next very significant chapter in this work is the security question, today very often mentioned. At first I was concerned with the physical security of the server against outside influences. In the next part I am dealing with the software security and how to apply all security elements to my server. Another chapter includes an analysis of the technical solution with economic aspects. Finally, this work includes testing webhosting solution that I proposed and compiled on my computer.

Key Words

Apache, computer security, hosting, Internet, ISPConfig, Linux, server, web, webhosting

Poděkování

Chtěl bych poděkovat všem, kteří se i malým dílem přispěli k tomu, že tato práce mohla vzniknout. Jmenovitě bych chtěl poděkovat mému konzultantovi Ing. Michalu Houšťovi za prvotní myšlenky na zpracování této práce. Dále bych chtěl poděkovat mému vedoucímu doc. Ing. Janu Skrbkovi, Dr. za postřehy během vypracování této práce a za čas věnovaný mi při konzultacích. A v neposlední řadě bych chtěl poděkovat celé svojí rodině za podporu, kterou mi dávala při psaní a shánění materiálů pro vypracování diplomové práce.

Obsah

Seznam zkratek a symbolů

BSD licence	pro svobodný SW, umožňuje volné šíření licencovaného obsahu
CGI	protokol pro propojení externích aplikací s webovým serverem
GNU GPL licence	pro svobodný SW, odvozená díla musí dostupná pod stejnou licencí
GUI	grafické uživatelské prostředí
IPv6	síťová vrstva pro přenos paketů, následovník IPv4
IT	informační technologie
URL	řetězec sloužící k specifikaci umístění dat na Internetu

Seznam tabulek

Seznam obrázků

1. Úvod

V dnešní době Internet tvoří nedílnou součást našich životů, ať se nám to líbí nebo ne. A využívání Internetu neustále stoupá ve všech směrech a sférách našich životů. Internet je celosvětová počítačová síť, díky které lze komunikovat, předávat nebo sdílet informace. Ale mnoho lidí si pod pojmem Internet představí webové stránky a služby s nimi spojené. Webové stránky se nacházejí na jednotlivých počítačích či serverech a my si je díky Internetu můžeme zobrazit. Webový server slouží jako prostor pro jednotlivé stránky a vzhledem k tomu, že ne každý chce provozovat server, vznikl pojem webhosting. Služba, poskytující webový prostor popř. další služby za určitou finanční částku. Proto jsem si vybral jako záměr této práce zjistit informace o webhostingu, jak vlastně funguje, co tato služba všechno obnáší. Tato problematika mě zajímá i z osobní stránky, vzhledem k tomu, že jsem začal pracovat ve společnosti zabývající se IT technologiemi a webhosting v sobě skrývá mnoho prvků, o kterých bych se rád dozvěděl více. Cílem této práce je shrnout současné možnosti realizace webhostingového řešení a vybrat nejvhodnější s ohledem na ekonomické aspekty.

Práce je rozdělena do jednotlivých částí odpovídajícím součástem dobře fungujícího webhostingového řešení. V jednotlivých kapitolách se zabývám výběrem vhodného operačního systému, webového serveru, databázového serveru a dalších prvků. Také se zabývám bezpečnostní analýzou, která je dnes téměř tou hlavní částí všech aplikací s přístupem do Internetu. Ve druhé části práce jsem testoval mnou vybrané řešení a některé výsledky jsem také zde také interpretoval.

2. Problematika poskytování webového prostoru.

V této kapitole bych chtěl čerpat z pohledu institucí, odborníků a lidí, kteří mají s touto problematikou zkušenosti. Jedná se převážně o kontroverzní téma v podobě právní souvislosti s poskytováním webového prostoru na síti Internet. Jinými slovy se jedná o právní odpovědnost za webhosting a služby s ním spojené. Podle doc. Smejkala [XXX] z VŠE se jedná hlavně o informační trestnou činnost, která spočívá v šíření informací a v shromažďování informací či dat. Majitel www stránek je přímo odpovědný za jejich obsah, který by měl být nezávadný. Jinými slovy, neměl by nijak porušovat zákony a platné normy daného státu. Jak ale tvrdí JUDr. Matejka [XIX] z Ústavu státu a práva akademie věd ČR, bohužel, řada otázek zůstává jak v právní teorii i praxi dosud neřešena. Zákony, které se touto problematikou zabývají, jsou: Zákon o elektronických komunikacích (Zákon č. 127/2005 Sb.), Zákon o některých službách informační společnosti (Zákon č. 480/2004 Sb.), Zákon o telekomunikacích (Zákon č. 151/2000 Sb.), atd.

JUDr. Matejka [XIX] zmiňuje několik základních pojmů, které je třeba zmínit a vysvětlit. Patří mezi ně cizí obsah. V našem případě se jedná o elektronická data, náležící jinému subjektu než poskytovateli webového prostoru. Tyto data lze přenášet pomocí elektronické komunikace a v některých případech i uchovávat na záznamových médiích. Další pojem je webový prostor. Jedná se datový prostor na Internetu, kde může být na základě smlouvy tento obsah zpřístupněn. A na závěr kdo je poskytovatel webového prostoru. Jedná se o právnickou nebo fyzickou osobu, která poskytuje daný webový prostor na Internetu jiným subjektům na základě smlouvy. Zároveň tak zpřístupňuje tento cizí materiál prostřednictvím sítě Internet dalším subjektům. Podle jeho tvrzení je poskytovatel webového prostoru odpovědný za cizí obsah, který mu je znám, popř. by mu měl být znám a je technicky schopen mít přístup k tomuto obsahu. Pokud naopak není technicky schopen přístupu k tomuto obsahu, pak poskytovatel webového prostoru neodpovídá za cizí obsah umístěný na webovém prostoru jím poskytnutý. Zákon (480/2004 Sb.) dále výslovně stanoví, že poskytoval webhostingu není povinen dohlížet na obsah ukládaných informací ani aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace. Další výjimka může nastat, pokud má poskytovatel přímý vliv na činnost uživatele. V tomto případě je plně zodpovědný za obsah, který uživatel na daný server ukládá. Ale ani v zákoně není toto přesně definováno, resp. řídí se dalšími okolnostmi, např. předmět činnosti. Uvedu příklad z praxe. Pokud webhostingový server spravuje tisíce stránek, je pro administrátora téměř nemožné kontrolovat jejich obsah.

Na druhou stranu, jedná-li se o server, zabývající se publikací videí, v dnešní době velmi populární server Youtube.com je zcela zřejmé, za jakým účelem byl vytvořen. Miliony uživatelů na celém světě zde mají možnost shlédnout obrovské množství videí bez jakékoliv registrace. K omezení či odstranění materiálů porušují práva a zákony dává pokyn soud či majitel práv k těmto materiálům. Proto občas na stránkách Youtube.com se objeví hláška, že video bylo odstraněno na pokyn společnosti např. BMG.

Pokud se podíváme na stanovisko Evropské unie, tak směrnice Evropského parlamentu a Rady č.2000/31/ES říká, pokud chce snížit svou odpovědnost, musí poskytovatel webhostingu, jakmile zjistí nebo se dozví o protiprávní činnosti na svém serveru přijmout veškerá opatření k odstranění daných informací nebo znemožnění přístupu k nim.

Na každý server se uplatňují pravidla země, ve které je daný server fyzicky umístěn a nezáleží, jaké případně používá domény. V praxi to znamená, že server umístěný v Praze a provozující webové stránky s koncovkou .com je posuzován podle zákonů České Republiky.

Z důvodů uvedených výše je nezbytné pro každého poskytovatele webového prostoru najít způsob, jak se vyhnout nepříjemnostem související s porušováním zákonů dané země. [XXX; XIX; IX]

2.1. Historie webu

World Wide Web neboli zkrácené www či web je projekt, který vznikal a vyvíjel se mnoho let. Všeobecně je web považován za nápad jednoho člověka – Tim Berners-Lee. V roce 1989 předložil Berners-Lee v Ženevě ve Švýcarsku ve výzkumném projektu CERN (Conseil Européen pour la Recherche Nucléaire) návrh, ve kterém nastínil systém založený na hypertextu. Tento návrh se ale nezabýval technickou stránkou systému a ani neřešil potřebu vývoje síťových protokolů pro podporu tohoto systému. Jeho návrh ani nijak počítal s rozšířením do globálních rozměrů, jakých web dosahuje dnes. V roce 1990 byla zakoupena pracovní stanice NeXT Cube a v CERNu začaly práce na prvním webovém prohlížeči. Postupně vznikala první webová sídla tvořená akademickými a výzkumnými institucemi a v roce 1992 jich bylo 26 na celém světě. Změna nastala v roce 1993, kdy CERN zpřístupnila svůj vlastní server společně s instrukcemi, jak jej přenášet a kompilovat pro různé druhy hardwaru. Ve Spojených Státech Amerických v National Center for Supercomputing Applications (NCSA) byl uvolněn k volné distribuci prohlížeč NCSA Mosaic a zároveň také spuštěn server NCSA httpd. Uvolnění tohoto prohlížeče znamenalo neočekávané a trvalé

zvyšování webových serverů na internetu. V roce 1995 založením Apache Group převzal roli nejpoužívanějšího serveru Apache, který je také nejvíce používaným serverem dnes[1]. Apache byl funkčně identický a spravoval se stejně jako httpd a stal se jeho plnohodnotnou náhradou bez potřeby úprav systémových nebo konfiguračních souborů. V dnešní době se nejvíce serverů vyvíjí a podporuje komerčně, jedná se hlavně o servery od společností Netscape a Microsoft. Ale na druhé straně, je tady stále volně dostupný server Apache, který obdržel od společnosti Gartner Research Group potvrzení o své spolehlivosti a bezpečnosti. A i díky tomuto ocenění stále více proniká Apache a Linux mezi 1000 největších firem na světě. [I]

2.2. Jak web funguje

Rychlost, s jakou se web rozšířil, je velmi často přičítána dosažitelnosti jeho technologie. V počátcích používání webu byly webové prohlížeče distribuovány zcela volně a to umožnilo rychlé rozšíření. Díky webovému informačnímu rozhraní máme přístup k odkazům na miliony sídel po celém světě. Díky tomu se nám otvírá velké množství informačních depozitářů často volně přístupných. Mezi hlavní důvody rozšíření webu rostoucí popularita, kombinace textu a barevné grafiky.

Mezi základní prvky webu patří hypertextový odkaz tzv. hyperlink. Díky odkazům na webových stránkách získáváme přístup k prostředkům nacházejícím se téměř kdekoliv na světě. Aby se toto mohlo realizovat, bylo vytvořeno několik částí webu. První byla metoda, sloužící k jedinečné definici každého webového prostředku, a byla nazvána URL (Uniform Resource Locator). Druhým faktorem bylo schéma formátování přenášených dokumentů. Tímto schématem je HTML (HyperText Markup Language). A jako třetí část bylo nezbytné vytvořit způsob pro spojení do jednoho informačního systému. Vznikl síťový komunikační protokol HTTP (HyperText Transfer Protocol) spojující klientské pracovní stanice s webovými servery.

URL jak již bylo řečeno, slouží k rozpoznání prostředku dostupného pomocí sítě internet. Skládá se ze tří částí. První je mechanismus pro získání prostředku, názvu hostitele serveru a názvu prostředku. URL dále zjistí HTTP jako protokol, který bude využit pro načtení daného souboru. Protokol HTTP patří mezi nejrozšířenější, o dalších se budu zmiňovat později. [I]

[1] (www.netcraft.com, 2009)

2.3. Co to je webhosting

Webhosting je poskytnutí diskového prostoru pro webovou prezentaci www stránek a dalších služeb. Webové stránky jsou zpravidla umístěny na výkonném, spolehlivém serveru, který je umístěn na dostatečně zabezpečeném místě s vysokou konektivitou k internetu.

Doména je služba umožňující zobrazení www stránek pomocí sítě Internet. Domény se rozdělují podle úrovní. První úroveň, tedy nejvyšší, jsou TLD (toplevel domény) nebo národní domény. Doména tohoto typu pro ČR je „.cz“ .Domény druhé úrovně jsou za národní doménou, např. „seznam.cz“. A konečně doména třetí úrovně, kterou může být např. „wap.seznam.cz“. [IV]

3. Analýza programového vybavení.

Pro úspěšný provoz webového serveru kromě hardwarového vybavení je nezbytné samozřejmě i softwarové vybavení, kterému se budu věnovat v následující kapitole. Do kategorie softwaru, který budu používat pro řešení web hostingové aplikace, patří operační systém, webový server, podpora pro e-mailovou aplikaci, podpora pro databázový software a také skriptovací programovací jazyk PHP. V následujících kapitolách si jednotlivé prvky rozebereme podrobně.

3.1. Webový server

Webový server se skládá ze dvou základních částí. Jedná se o hardwarové a softwarové vybavení. Hardwarovým vybavením se budu zabývat v kapitole 5, týkající se technického řešení a ekonomických aspektů.

Webový server je program, který používá model klient/server a protokol HTTP k zajištění přenosu souborů z webových stránek k uživatelům používajících webový prohlížeč, který přijímá jejich požadavky. Odpovědí na tento požadavek bývá zpravidla HTML dokument, či dokument v jiném formátu (text, obrázek, apod.). Mezi další funkce webového serveru patří ověřování uživatelů a šifrování dat, přístup k databázím (není potřeba speciální aplikace databázového klienta), atd.

3.1.1. Hlavní hráči

Funkci webového serveru může plnit téměř každý software, který implementuje http, můžeme nalézt poměrně hodně různých druhů webových serverů, které se dnes používají. Můžeme nalézt servery, které představují zcela vlastní a jedinečná řešení. Většinu z nich rozpoznáme a identifikujeme pomocí konkrétního názvu a verze. I když je zde velký počtu serverů HTTP tak se jen málo z nich podílí na většině provozu HTTP na internetu. V následující tabulce můžeme vidět podíl jednotlivých společností a serverů v únoru 2009. [IV]

Tab. 1 - Podíl serverů na trhu – únor 2009

Server	Počet serverů	Procentní podíl (%)
Apache	26,636,952	71,94
Microsoft	6,470,899	17,48
Zeus	122,631	0,33
Netscape	38,140	0,1
WebSTAR	12,635	0,03
WebSite	5,692	0,02
Ostatní	3,737,962	10,1

Zdroj:*http://www.securityspace.com/s_survey/data/200902/index.html ,9.3.2009*

3.1.2.Servery zdarma (open-source)

Některé z nejlepších webových serverů jsou zdarma. Apache je volně šiřitelný open-source software. Kořeny webu (protokoly, prohlížeče a servery) pocházejí z volně šířeného a otevřeného akademického prostředí. Volně šířené servery CERN a NCSA započaly revoluci webu a i když žádný z nich dnes již není životaschopný, některé druhy softwaru pro servery udržují tuto tradici volné dostupnosti až do dnešního dne. [IV]

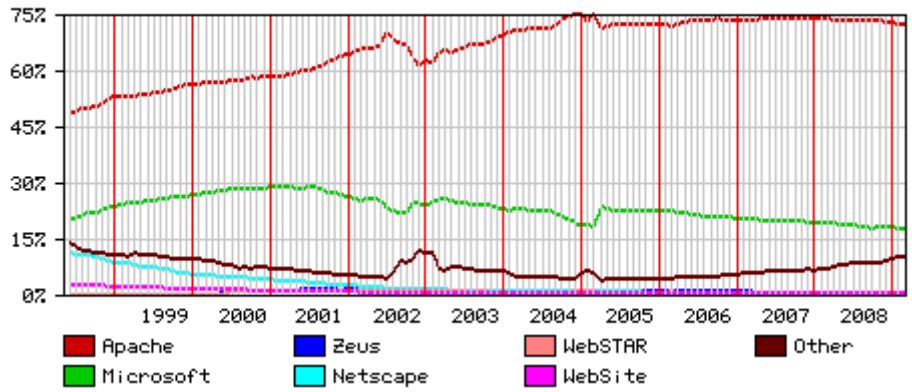
3.1.2.1. Apache

Server Apache je dlouhodobě nejrozšířenější webový server, který lze použít na různých platformách operačních systémů. Jedná se o webový server s otevřeným kódem, takzvaný open-source software. Vývoj tohoto serveru začal v roce 1993 v National Center for Supercomputing Aplications (NCSA) na univerzitě v Illinois. V únoru 1995 vznikla Apache Group, skupina vývojářů, díky které vznikl modifikací původního kódu nový volně šiřitelný server. Postupně k němu byly přidávány záplaty (patches), které zvyšovaly funkčnost a stabilitu serveru a daly tak i podnět k pojmenování nového serveru na Apache.

Název vznikl z úcty a obdivu k domorodému kmenu nativních Američanů - Apačů a anglického slovního spojení „A patchy server“ (patchovaný server, kdysi byl Apache pouze sada patchů pro jiný web server). Jako indiánský symbol je ve znaku ptačí pero.

Od dubna 1996 byl Apache nejpopulárnější server na internetu. V květnu 1999 běžel na 57 % všech serverů a v listopadu 2008 jeho používanost dosáhla 74 % (výsledky měření securityspace.com).

Obr. 1 - Podíl serverů na trhu 1999 – 2008



Zdroj: *http://www.securityspace.com/s_survey/data/200902/index.html ,9.3.2009*

3.1.2.2. Thttpd

Jedním z nejzajímavějších volně dostupných serverů http je produkt jednoduše nazývaný thttpd. Jeho výhodou je, že je navržen tak, aby byl extrémně rychlý, měl malé nároky na paměť, byl jednoduše instalovatelný, spravovatelný a vysoce bezpečný. Ale jeho velkou nevýhodou je absence dalších funkcí a navíc při extrémní zátěži vypadává.

Server kromě standardních vlastností podporovaných i jinými webovými servery implementuje několik velmi specifických vlastností. Jednou z nich je např. tzv. URL based throttling, který umožňuje limitovat odchozí provoz v závislosti na URL. Samozřejmostí je i nativní podpora IPv6 bez nutnosti aplikace externích záplat.

3.1.2.3. Mathopd

Tento server je k dispozici pouze pro operační systémy Unix a Linux. Jeho kód je navržen tak, aby byl schopný zpracovat velmi velký počet souběžných připojení. Je to velmi rychlý webový server díky používání systémového volání *select()* systému Unix, které používá pro zpracování více spojení s klienty místo spouštění více procesů nebo vláken. Díky jednoduché instalaci, nastavení a optimalizaci pro maximální možnou rychlost v poskytování statických stránek velkému počtu připojujících se klientů vypadal Mathopd jako velmi atraktivní alternativa Apache. Bohužel ale Mathopd neumožňuje ověřování uživatelů, zabezpečená spojení nebo podporu programování.

3.1.2.4. Boa

Tento server je určen převážně pro správce, kteří jsou ochotni obětovat některé funkce, aby dosáhli vyšší rychlosti a bezpečnosti. Požívá také systémové volání select() pro paralelní zpracování vstupu a výstupu. To znamená, že při příchodu nového požadavku nezakládá nový proces, ale interně se rozdělí mezi všechny požadavky. Velmi dobře zvládá velký počet skriptů CGI, asi nejvíce ze všech serverů běžících na operačním systému Linux. Tato výhoda je dána tím, že Boa posílá výstup skriptů CGI přímo ke klientovi. Většina ostatních serverů přijímají datový výstup z programů CGI a pak jej odesílají webovému klientovi (prohlížeči).

3.1.2.5. Planet (Sun Java System Web Server)

Tento server byl velmi dlouho znám pod názvem Netscape Enterprise Server, ale byl přejmenován, když America Online (vlastník Netscape Communications) a Sun vytvořili alianci Sun-Netscape. Když tato aliance zanikla iPlanet se stal divizí společnosti Sun. Jeho vytvoření se datuje k roku 1999. Tento server je k dispozici pro většinu operačních systémů (MS Windows, Linux, IBM AIX…) a vyznačuje se vysokou úrovní efektivnosti, spolehlivosti a možností správy. Tento server je založen na platformě Java. To znamená, že vyžaduje „java-enabled server“, JVM (Java Virtual Machine) a také JavaServer Pages technologii. Tento server podporuje PHP, ColdFusion a CGI.

3.1.2.6. Roxen Challenger

Roxen Webserver je dílo švédské společnosti Roxen Internet Sofrware. Jedná se o plně vybavený webový server, který je šířen pod GPL licencí. Běží na mnoha různých operačních systémech, včetně MS Windows, Linux, Solaris a Mac OS. Mezi jeho silné stránky patří online rozhraní pro snadnou konfiguraci a správu, grafická podpora pro generování např. hlaviček, obrázků a grafů, integrovaná databáze MySQL, podpora programovacích jazyků Java, Perl, PHP, modulární architektura (serverové rozšířené mohou být nahrány bez vypnutí procesů běžících na serveru). Tento webový server je sice šířen jako open-source software, ale na rozdíl od serveru Apache je součástí nástrojů nazývaných Roxen Platform a ta je již zpoplatněna. Takže bez drahých vývojářských nástrojů nenabízí žádnou výhodu oproti Apache, který je mnohem používanější a díky tomu i podporovanější.

3.1.3. Komerční servery

Komerční webové servery byly vytvořeny na požadavek společností a firem, které tento software vyžadují. Na druhou stranu ne vždy může být komerční software kvalitnější či mít lepší podporu než open-source software.

Hlavní motivací pro komerční cestu je podpora nabízená dodavatelem. Při využití komerčního softwaru by měl uživatel co nejvíce využít všech služeb, které dodavatel nabízí. Ať už se jedná o pomoc při zavádění a spouštění webového sídla, či nastavení veškerého zabezpečení a hlavně o celková servis spojený s provozem webového serveru. Mnoho produktů z komerčního prostředí je ale odvozeno od open-source softwaru s různými dalšími úpravami zdrojového kódu. [I]

3.1.3.1. Stronghold

Tento webový server byl vyvinut společností Red Hat a jedná se o server Apache doplněný o silnou podporu SSL. Tento produkt je prodáván jako plně připraven k instalaci a samozřejmostí je podpora dodavatele. Stronghold je možné si vytvořit z volně šiřitelného serveru Apache, ale je potřeba mnoho času a zkušeností, a proto většina firem vyžadující vysoké zabezpečení sáhne již po připravené verzi Stronghold. Základní cena se pohybuje od $349[2].

3.1.3.2. Zeus

Zeus Web Server je webový server pro Unix a Unix-platformy, jako je (v současné době Solaris, FreeBSD, HP-UX a Linux). Podpora pro AIX, Tru64 a Mac OS X byla vypuštěna 10. června 2008 (www.zeus.com). Tento server byl vyvinut společností Zeus Technology, která se nachází ve městě Cambridge ve Velké Británii. Původními autory a zakladatelé Zeus Technology byli studenti tamní univerzity Damian Reeves a Adam Twiss.

Tento webový server se používá převážně v oblasti bankovním, finančním a obchodním sektoru. Zeus i se svým malým podílem na trhu je poměrně velkým konkurentem serveru Apache, pokud je zákazník ochoten vynaložit na něj finanční prostředky. Jeho cena se pohybuje okolo $1700[3]. Zeus má velmi dobře vyřešenou otázku zabezpečení (je odolný vůči všem známým DoS útokům a využívá také SSL šifrování), což je ve výše zmíněných sektorech jedna ze základních podmínek. Pomocí svého integrovaného rozhraní umožňuje

[2] (www.redhat.com, 17.3.2009)
[3] (www.pcmag.com, 19.3.2009)

rychlé a jednoduché generování certifikátů na klientovi a podobně jako Apache poskytuje podporu pro hardwarové kryptografické urychlovače. Zeus na rozdíl od Apache poskytuje zabudovanou analýzu hrozeb v reálném čase.

3.1.3.3. IBM

IBM HTTP Server je sice k dispozici zdarma, ale bez jakékoliv podpory ze strany IBM. Pokud by zákazník požadoval podporu, je nutno zakoupit IBM WebSphere Application Server, který je již zpoplatněn. Tento server od společnosti IBM je k dispozici pro většinu operačních systému, mimo jiné AIX, HP-UX, Linux, Solaris a Windows. IBM server je založen na jádru serveru Apache a IBM k němu jen přidala několik dalších funkcí. IBM zaručuje veškerou kompatibilitu s Apache, proto moduly kompilované pro webový server Apache fungují i na IBM serveru. Pokud uživatel vyžaduje vysokou podporu a asistenci pro svůj server, je pro něj IBM vhodným řešením. IBM HTTP server funguje pouze na hardwaru od společnosti IBM.

3.1.3.4. Microsoft IIS

Nejdříve bych uvedl větu, kterou pronesl programátor a administrátor Unixu Mike Huck ze společnosti Amazon.com.

Co mě děsí, je proč lidé investují tolik peněz do NT, když existuje tolik důkazů, že Unixy jsou vyspělejší, stabilnější, levnější a o tolik výkonnější! Proč? Co se těm lidem děje? [4]

Microsoft Internet Information Server je poskytován jako součást balíku NT Option Pack a systému Windows 2000 Server, a pro jeho provozování je nutné si zakoupit jeden z těchto OS. Nejnovější verzí je IIS7, která se vyznačuje stejně jako Apache samostatnými knihovnami neboli moduly, které lze přidávat či podle potřeb správce a zákazníka. IIS7 používá konfigurační model známý z ASP.NET, to znamená hierarchicky organizované XML soubory. Oproti předchozím verzím má také tato verze lepší konfigurační nástroje. Nová generace IIS Manageru je přehlednější a schopnější. Mimo jiné též umožňuje z jednoho místa provádět konfiguraci vlastností serveru i nastavení aplikace. V IIS7 je nové lepší GUI pro administraci. Má být tímto do jisté míry spojena konfigurace IIS a .NET aplikací. [XI; XXXIII]

[4] Microsoft Windows NT Server 4.0 versus UNIX, [online], Huck Mike, 1999, [cit. 2009-03-25]. Dostupný z WWW: http://www.penguin.cz/~had/unix-nt/

3.1.4.Proč Apache?

V roce 2008 provedl server Root.cz analýzu českých serverů hostujících webové stránky a zjistil, že server Apache se vyskytuje na cca. 88%[5] serverů. Toto vysoké číslo svědčí o popularitě serveru Apache. V celosvětovém měřítku je Apache rovněž nejrozšířenější server a podle serveru Netcraft.com zaujímá cca. 46,6%[6] trhu, na druhém místě je podle serveru Netcraft.com Microsoft s podílem 21,9%[7]. [XIII]

Apache je díky své rozšířenosti server, který se těší velké popularitě z řad odborníků, ale i nadšenců, kteří si své názory, zkušenosti a informace sdělují na různých fórech a i díky tomu má Apache velmi dobrou podporu na rozdíl od některých dalších serverů. Apache vyniká svojí rychlostí, mnoha funkcemi a spoluprácí s mnoha operačními systémy, ale nejlépe s Linuxem.

Další faktor, který hovoří pro Apache, je licence. Jedná se o svobodný software, který je distribuovaný zdarma.

3.1.4.1. Vlastnosti Apache

Webový server Apache je jedním z nejvíce univerzálních serverů na dnešním internetu. Díky své flexibilitě je také nejrozšířenější, o čemž svědčí internetové průzkumy (netcraft.com a securityspace.com). Apache nabízí velké množství prvků zahrnující virtuální hostování podle názvů nebo IP adres, ověřování uživatelů, přepisování URL, Server Side Include (SSI), pokročilé logování, proměnné prostředí, vyjednávání obsahu, rozhraní Common Gateway Interface (CGI), Secure Sockets Layer (SSL) a ještě mnohem více.

3.1.4.2. Architektura Apache

Architektura serveru Apache je tvořena několika vrstvami jak můžeme vidět na obrázku. Nejnižší vrstva je tvořena operačním systémem. Pro server Apache je nejčastější představitel operační systém Unix a Linux, ale server Apache spolupracuje i s MS Windows, MacOS, BSD aj. Základní vrstvou je jádro, které zajišťuje funkcionalitu a zodpovídá za komunikaci s operačním systémem a komunikaci se síťovým prostředím. Na obrázku je tato vrstva označena číslem dvě. Tato vrstva, jak již bylo řečeno, se skládá z jádra, dále z vestavěných modulů a několika standardních knihoven. Jádro spolu s modulem http_core zajišťuje

[5] Root.cz, 21. 7. 2008
[6] Necraft.com, září 2009
[7] Necraft.com, září 2009

základní funkcionalitu a propojení API (Aplication Programming Interface) se třetí vrstvou tvořenou moduly. Vrstva modulů rozšiřuje funkce serveru Apache o další možnosti. Pro základní funkčnost není tato třetí vrstva vyžadována. Architektura může být doplněna ještě o jednu vrstvu, v pořadí již o čtvrtou. Tato vrstva může být prázdná nebo může obsahovat další moduly pro rozšíření funkčnosti serveru Apache. [XXII]

3.2. Operační systém

Operační systém je základní softwarové vybavení počítače, které se stará o správu systémových zdrojů. [8]

Operační systém je rozhraní, které umožňuje uživateli komunikovat s hardwarem počítače. V 70. letech došlo ke vzniku dvou dnes již legendárních operačních systémů. První z nich, VMS, vytvořila pro své počítače VAX firma DEC. Tím druhým byl ještě slavnější UNIX firmy AT&T. Protože byla tato firma v rámci antimonopolního řízení americké vlády nucena zříct se své počítačové divize, převedla UNIX za velmi výhodných podmínek na některé univerzity. Vznikla tak varianta BSD (Berkeley System Distribution). Poté vznikaly další verze Unixu, ať už založené na základech systému firmy AT&T nebo na BSD. Vznikl např. IBM AIX, HP-UX, SGI IRIX, Cray Unicos, Sun Solaris a další. Všechno to však byly operační systémy pro sálové počítače nebo minipočítače. Počátek operačních systémů pro PC se datuje na začátek osmdesátých let, kdy společnost IBM vytvořila první osobní počítač typu PC. Tento počítač používal systém DOS od společnosti Microsoft. I když měl tento systém mnoho nedostatků a omezení, byl však okamžitě k dispozici. Počítač se ovládal pomocí příkazů v textovém režimu. Příkazy se vkládaly do textového řádku. Později se již objevilo grafické uživatelské rozhraní na počítačích od společnosti Apple (v roce 1984). Zatímco třeba společnost Microsoft přišla s grafickým prostředím až v roce 1992, kdy uvedla na trh Windows 3.1. Grafické rozhraní potom umožňovalo uživateli ovládat počítač pomocí myši a ikon představující objekty a aplikace v počítači. Ve světě velkých počítačů, pracovních stanic a síťových serverů panoval Unix, ať už měl jakékoliv jméno a byl od kterékoliv firmy. Unix se také vyvíjel, paradoxně hlavně díky tomu, že nebyl zadarmo. Díky rozmachu Internetu a vzniku internetových komunit, složených z mladých lidí, programátorů, kteří hledali co nejlevnější a nejefektivnější způsob komunikace a práce, obrátili se směrem k Unixu. Museli přepsat celý systém znovu od začátku a vytvořit Unix pro PC, který byl nejrozšířenější

[8] Vychodil V., *Linux Příručka českého uživatele*, Brno: Computer Press, 2003. 260s ISBN 8072263331

platformou. Bylo využíváno systém BSD a vznikly verze pro PC, např. FreeBSD, OpenBSD či NetBSD. Následně se objevil systém Linux šířený pod licencí GPL (General Public Licence). Mezi další systémy lze zmínit BeOS, také založený na systému Unix. O jednotlivých operačních systémech jsou následující kapitoly. [XII]

3.2.1.Linux

Linux vznikl v roce 1991 jako projekt finského studenta Linuse Torvaldse, kterému nebyl dostatečný systém Minux (malý Unix) vytvořený pro stroje Intel386. Jeho první verzí byla 0.02 a již od počátku neobsahovaly zdrojové kódy žádný kód z původního systému. Vývoj Linuxu neustále pokračuje a vydávají se stále novější verze. Linus Torvalds je také autorem loga Linuxu, tučňáka Tuxe.

Operační systém Linux vychází z koncepce Unixu a je kompatibilní s ostatními implementacemi systému Unix na úrovni zdrojového kódu.

Operační systém Linux je znám zejména svou rychlostí, minimálními hardwarovými požadavky, bezpečností a vzdálenou správou. S Linuxem se lze setkat od kapesních počítačů, přes pracovní stanice a servery, až po počítače třídy mainframe. Linux je plně vybavený operační systém, který je k dispozici zdarma. Jádro operačního systému Linux je k dispozici pod všeobecnou veřejnou licencí (General Public License – GPL) GNU. Správně by se tedy celý systém měl jmenovat GNU/Linux. Protože Linux je pouze jádro operačního systému. Díky licenci GNU má každý uživatel právo software upravovat a dále šířit za předpokladu poskytnutí i zdrojového kódu.

Další výhodou Linuxu je jeho schopnost běžet s grafickým prostředím (GUI) nebo bez něj. Záleží na požadavcích uživatele.

Linux je víceúlohový systém. V praxi to znamená, že každé úloze na základě její priority je přidělen určitý procesorový čas, který využije a ihned přijde na řadu další proces. Díky nízkým časovým intervalům se pro lidského pozorovatele jeví tento systém jako by běželo více úloh současně.

Systém Linux je rovněž navržen jako víceuživatelský. To znamená, že může současně pracovat více uživatelů, aniž by se nějakým způsobem ovlivňovali nebo si překáželi. [XXV; XXXIV]

Systém Linux je možno získat několika způsoby. V prvním případě si uživatel může stáhnout jednotlivé balíčky zdrojového kódu a systém si zkompilovat. Což ale může být poměrně složité a náročné. Většina uživatelů získá Linux jako distribuci od konkrétního výrobce. Tato cesta je rychlá a jednoduchá. Pokud uživatel zaplatí za CD s konkrétní distribucí, získá také potřebnou dokumentaci a většinou i určitou úroveň technické podpory.

3.2.1.1. Distribuce Linuxu

V následující kapitole se budu věnovat nejznámějším a nejpoužívanějším distribucím Linuxu. Celá tato kapitola včetně podkapitol byla volně citována z [XXIII].

- Fedora

Tato distribuce vznikla jako nekomerční část distribuce Red Hat Linuxu za podpory firmy Red Hat. Díky Fedoře může Red Hat připravovat svojí komerční distribuci Red Hat Enterprise Linux. Fedora je především známá svými inovacemi a novinkami v každé verzi. Je zaměřena na použití na osobních počítačích.

- Mandriva

Mandriva Linux vznikla v roce 1998 jako Mandrake. Je určena především pro uživatele kancelářských aplikací a multimédií. Vyniká svou komplexností a snadnou správou. Mezi hlavní výhody patří rychlá instalace a snadné základní nastavení, proto je také oblíbená mezi začínajícími uživateli. Mandrivu můžeme dostat v několika verzích. Od placené krabicové verze až po verzi zcela zdarma. Rozdíl je tvořen především rozsahem dokumentace, doplňků a komerčních aplikací.

- Suse

Tato distribuce patří mezi ty starší, byla uvedena v roce 1994 jako S.uS.E Linux 1.0 . Dříve byly vydávány tři verze (Professional, Personal a Live Eval), dnes je k dispozici jedna volně dostupná verze a potom verze určené pro serverová řešení, ale k nim je doporučováno zakoupení aktualizací s platností jednoho roku.

- Gentoo

Tato distribuce je určena již pro pokročilejší uživatele. Umožňuje totiž velkou pružnost při instalaci systému (sestavení na míru-kontrola nad balíčky které budou nainstalovány a které

ne). Díky této vlastnosti je gentoo označované za metadistribuci. Gentoo je velmi dobře dokumentována a poskytuje pokročilejším uživatelům možnost dalšího rozvoje jejich znalostí o Linuxu.

- Debian

Debian patří mezi nejrozsáhlejší distribuce. Je plně vyvíjena komunitou a podporuje jedenáct platforem. Tato distribuce nemusí být nutně založena na jádru Linux, ale používá také jádra FreeBSD a NetBSD. Debian má specifický vývojový cykl. Má tři části: stable, testing a unstable. Stable je víceméně neměnný, jen se do něj přidávají opravy a záplaty. Na dalších dvou se provádí vlastní vývoj. Z testing verze se stává stable, a z unstable potom testing. Mezi silné stránky Debianu patří jeho balíčkovací systém apt, o kterém uživatelé tvrdí, že je nejlepším balíčkovacím systémem vůbec.

- Ubuntu

Je to poměrně nová distribuce, její první verze vyšla v roce 2004. Je postavena na distribuci Debian GNU/Linux a podporována firmou Canonical. Cílem Ubuntu je přiblížit Linux uživatelům na osobních počítačích. Ale je samozřejmě vhodný i pro serverové řešení. Ubuntu obsahuje více než 16 000 programů, ale základní instalace se vejde na jedno CD. Ubuntu pokrývá každou běžnou aplikaci od textových editorů a tabulkových procesorů přes aplikace pro přístup k internetu, webový server, e-mail, programovací jazyky a nástroje.

3.2.2. MS Windows

Historie Microsoft Windows začíná kolem roku 1981, kdy spolu s prvním osobním počítačem byl distribuován systém MS-DOS. Díky společnosti IBM, která umožnila výrobu klonů svých počítačů, se rozšířil i systém MS-DOS. MS-DOS byl ale už v době svého uvedení velmi nepohodlný. Umožňoval pouze jednoho připojeného uživatele, chyběla podpora multitaskingu a měl hardwarová omezení. Tyto nedostatky byly později nahrazeny dalšími verzemi MS Windows. Komerčního úspěchu dosáhla ale až verze Windows 3.0 vydaná v roce 1990. Již nabízela hardwarovou a softwarou podporu mnoha nezávislých výrobců, dále grafické prostředí GUI a rychle se rozšiřovaly díky přeinstalování na nových PC. Mezi dalšími verzemi stojí za zmínku Windows 3.1 a 3.11 kde již byla přidána síťová podpora. V roce 1995 byly uvedeny na trh Windows 95, který měl již částečně 32bitové jádro (hybridní 16/32bitové). Dále se objevila integrace protokolu TCP/IP, nové grafické prostředí GUI.

Tento systém byl označen jak „user friendly“ , což znamená uživatelsky přívětivý. Pak již následoval plně 32bitový systém Windows 98 s vylepšeným grafickým prostředím, plně funkční podporu USB, nový Microsoft Explorer 4. Bohužel systém obsahoval mnoho chyb a byl velmi nestabilní. Na to zareagoval Microsoft a vydal Windows 98 SE, který byl stabilnější a kvalitnější systém. Všechny systémy byly postaveny na jádře pracujícím pod DOSem a jako poslední z této kategorie byl Windows ME, který kromě toho, že přinesl několik vylepšení, bývá označován za nejméně stabilní systém od Microsoftu. V roce 2001 byl uveden na trh systém, který nebyl postavený na DOSu, s názvem Windows XP (jednalo se o 64bitový systém). Tento systém se pyšnil spolehlivostí a také zpětnou kompatibilitou i s verzemi NT. Objevila se podpora multimedií a také skinovatelnost grafického prostředí. Rovněž se zkrátil spouštěcí čas oproti minulým verzím. Další verzí jsou Windows Vista vydané na začátku roku 2007. U tohoto systému se Microsoft inspiroval u operačního systému Mac OS a zavedl grafické rozhranní nazvané Aero. Další novinkou bylo vyhledávání fungující na principu indexování souborů, úplnější podpora IPv6 a již zmíněné grafické prostředí.

Vedle systémů založených na DOSu se také vyvíjel systém nezatížený nedostatky DOSu a sice OS/2. Microsoft po rozpadu spolupráce se společností IBM přejmenovává svojí verzi na Windows NT (1993). Tento systém je převážně zaměřen na náročné uživatele a servery. Postupně vyšlo několik verzí Windows NT a v roce 2000 došlo ke změně názvu a svět spatřil MS Windows 2000. V roce 2003 představený Windows Server 2003 je čistě serverovým produktem (není dostupný jako Workstation) a k jeho vlastnostem patří zejména propracovanější bezpečnost, lepší robustnost a správa systémů. Je základem pro další celou rodinu serverových produktů Microsoftu.

OS Windows je dnes zejména díky masivním marketingovým kampaním a podpoře nezávislých výrobců HW v 90. letech nejrozšířenějším OS v oblasti kancelářských počítačů (bez ohledu na jeho nedostatky byl prosazen proti jeho často technologicky vyspělejším konkurentům). Systémy Windows různých verzí jsou instalovány na cca 90% všech kancelářských počítačů. [XVI]

3.2.3.Mac OS – operační systém počítačů Apple

Počátky systému Mac OS se datují k polovině devadesátých let dvacátého století. V tu dobu vydal Microsoft Windows 95 (byl na svou dobu uživatelsky příjemný) a na druhé straně Unix vynikal svojí stabilitou. A Apple začal trochu dech. Bylo vyzkoušeno několik projektů BeOS, Pink, Copland, TalOS, A/UX. Za bližší zmínku stojí projekt Copland, který přinesl několik desénových prvků, jež byly použity i v dalších Mac OS X. Měl skutečné mikrojádro a hardwarovou abstrakci, ale bohužel vývojáři nakonec nebyli schopni dodat fungující prototyp systému, a proto byl projekt ukončen. Systém BeOS byl multimediální systém s podporou meta-dat na úrovni file systému, grafickým rozhranním, preemptivním multitaskingem. Systém ztroskotal na vysoké ceně, kterou společnost Be požadovala na společnosti Apple. Podobně dopadly i ostatní projekty, buď byl jejich vývoj zastaven, nebo projekt koupila jiná společnost, jako např. TalOS společností IBM. V roce 1997 byl Apple koupen společností NeXT, kterou vlastnil původní zakladatel firmy Apple, Steve Paul Jobs. Byl vyvinut systém Mac OS X Server 1.0, který se skládal ze systému společnosti NeXT jménem Rhapsody, z původního Mac OS a několika unixových technologií. V roce 2001 byla vydána finální verze uživatelsky orientovaného systému nazvaná Mac OS C 10.0 Cheetah. Od této doby vychází Mac OS X přibližně v ročním intervalu. Po verzi Cheetah vyšla verze Puma, celým označením Mac OS X 10.1, která přinesla nárůst výkonu a stability, ale pořád měla daleko ke skutečně kvalitnímu systému. Tím se stal až Max OS X 10.2 Jaguar. Bylo zde značné zlepšení stability a díky OpenGL akceleraci správce oken i citelné zrychlení. A konečně verze Panther je považována za první „dospělý“ Mac OS. Kromě už perfektní stability a rychlosti obsahuje řadu vylepšení uživatelského interface a funkcí systému.

Základem Mac OS je mikrojádro Mach 4.0, které se stará o základní komunikaci s Open Firmware nebo BIOS (záleží na platformě), správu paměti, vláken a procesů, atd. Mikrojádro je obaleno klasickým BSD kernelem. Mach a BSD tvoří dohromady unixové jádro zvané XNU(XNU´s Not Unix). Kompletní systém, jehož součástí je více jak 250 částí, se nazývá Darwin. Ten je dodáván včetně velkého výberu BSD a GNU nástrojů, Apache, PHP a kompilátoru gcc. Systém je vydáván pod licencí APL (Apple Public Licence) či GPL licencí. Rozdíly oproti Linuxu jsou např. Linux vychází z větve Unixu zvané Systém V, zatímco Darwin vychází z BSD. Mac OS rovněž neobsahuje linuxové run levely, v kořenovém adresáři se nachází mach_kernel, atd. Pokud to tedy shrneme, tak Mac OS X je hybrid mezi BSD a GNU s trochou vlastní technologie.

Ještě bych se chtěl zmínit o několika službách, které jsou typické pro Mac OS X. Jedná se o framework Cocoa a Applovskou implementaci Javy a OpenGL.

Framework Cocoa vychází z NeXTStepu a jedná se o víceúrovňové API zajišťující snadný a rychlý přístup k určené podmnožině funkcí systému, stejně jako jednoduché propojení s dalšími systémovými knihovnami a frameworky. Aplikace využívající Cocoa mohou být napsány v Objective C nebo v Javě, a pokud jim nestačí kakaové funkce, mohou přistupovat i ke Carbon API a dalším součástem systému.

Apple si vyvinul svou verzi Javy sám a začlenil ji rovnou do nízkoúrovňových součástí Mac OS X. V systému najdete Javu 2 Standard Edition ve verzi 1.4.2 včetně Java Developer Kitu integrovaného do vývojového prostředí XCode. Javové aplikace mají přístup k objektovému frameworku Cocoa, mohou exportovat akce do Apple Scriptu (a tedy i Automatoru), vypadají stejně jako nativní programy, a pokud si zrovna samy neimplementují kdeco, ani nepoznáte, že děláte s Java Virtual Machine. Java aplikace se také chovají podle accessibility pravidel, podporují macovské Services i hlasové ovládání či čtení textu.

Grafická knihovna OpenGL je na většině operačních systémů implementována převážně výrobcem grafického hardware; Apple ale s firmami Ati a nVidia, které mu dodávají grafické karty na implementaci spolupracuje. V rámci této spolupráce výrobce karty připraví nejnižší úroveň ovladačů a firmware karty, ale veškerou návaznost na operační systém samotný řeší inženýři Apple. Tímto způsobem zniká jedinečná implementace, která na jedné straně nabízí stejnou verzi knihovny a podporu extensions a na straně druhé poskytuje systému nízkoúrovňovou kontrolu nad vším, co se děje s grafickým železem. [XXXI]

3.2.4. Další operační systémy

Kromě výše zmíněných OS jsou na trhu i další více či méně úspěšné projekty, zmíním se hlavně o BSD a Solaris.

- BSD

Berkeley Software Distribution je odvozen, (jak již název napovídá), od Unixu distribuovaného Kalifornskou univerzitou v Berkeley. Systém byl poprvé nainstalován v roce 1974 a byl používán pro rozsáhlý výzkum na univerzitě. Později se o tento systém začal zajímat i další univerzity a došlo k jeho distribuci pod označením 1BSD. Postupně byly

vydávány další verze až po verzi 4.4, resp. 4.4-Lite2 která se poté rozdělila na Free BSD (zaměřen na rychlost a podporu neserverového hardware), Net BSD (podpora různých architektur procesorů) a Open BSD (zaměřeno na bezpečnost). A mnoho dalších OS začlenilo kód odvozený z BSD do svého systému. Šlo například o MS Windows (implementace TCP/IP), Mac OS je částečně odvozen z kódu BSD či Solaris.

- Solaris

Solaris je operační systém vyvíjený společností Sun Microsystem. K dispozici je ve dvou verzích. Verze komerční a Open OS převážně určena pro studenty, Web 2.0 vývojáře a pro open source vývojáře. Je to operační systém unixového typu. Původně byl navržen pouze pro počítače s architekturou SPARC (jedná se o technologii, která byla vyvinuta společností Sun Microsystems). OS Solaris nabízí poměrně stabilní verzi, nezabugovaného operačního systému. Solaris se tváří a vypadá jako jedna z tradičních distribucí Linuxu, ale rozdíly najdeme „pod pokličkou“. Solaris používá jako souborový systém nazvaný ZFS (Zettabyte File Systém). Tento systém zvládne adresovat velké množství dat na dnešní dobu. Umožňuje vytvářet si obrazy z disku a nemusíte se bát práce s počítačem. To znamená, že v případě smazání nějakých dat není velkým problémem je znovu obnovit. Solaris nabízí i další prvky oproti jiným systémům, např. Storage Pool (umožňuje libovolné přidávání a odebírání disků), DTrace (umožňuje neustálou kontrolu všeho co počítač provádí), atd.

3.2.5. Proč Linux?

Proč jsem jako operační systém zvolil Linux?! Hlavním aspektem je jeho licence, která je koncipována jako dostupná pro všechny. Jedná se o tzv. GNU projekt. GNU licence zaručuje používání programu za jakýmkoliv účelem, možnost přizpůsobit ho svým potřebám, redistribuovat kopie programu, vylepšovat program a zveřejňovat zlepšení pro prospěch celé komunity. Další aspekt byl podpora a příslušná dokumentace. Linux používá a pracuje s ním velké množství lidí na celém světě včetně mnoha odborníků, kteří se velmi ochotně dělí o nabyté zkušenosti a informace. Většinu řešených problémů lze nalézt na webu, popř. se o nich poradit na fórech k tomu určených. Na Linuxu je možné rovněž pracovat vzdálené pomocí webového (HTTP) nebo souborového (FTP) serveru. Linux rovněž nabízí víceuživatelský a víceúlohový systém, který umožňuje práci více lidí najednou. Linux je také velmi variabilní, lze ho použít na velkém množství zařízení od PDA, přes notebooky a desktopy až po specializované servery. Výhodou Linuxu je, že se stále jedná o principiálně stejný systém a

není potřeba se učit novému zacházení. A v neposlední řadě Linux se projevuje jako velmi bezpečný systém bez virů a spywaru, neboť je velmi dobře zkompilován a odolává mnoha bezpečnostním komplikacím.

3.3. Elektronická pošta = E-mail

Elektronická pošta zkráceně e-mail je jeden ze základních komunikačních prostředků pro elektronický obchod ale i zábavu a jiný business provozovaný pomocí internetu. Historicky první emailová zpráva byla poslána v roce 1971 technikem Rayem Tomlinsonem. Do té doby bylo možno posílat e-mail pouze uživatelům, kteří se připojovali na stejný počítač jako odesílatel. Ray Tomlinson zavedl symbol @ jako pomocný identifikátor pro určení uživatele a počítače resp. domény (např. uživatelské_jméno@nějaké_místo.com). E-mailová zpráva se skládá ze tří částí:

- **Hlavička** – zpravidla obsahuje informace o typu e-mailu, adresáta, odesílatele,
- **Tělo e-mailu** – je to vlastní textová zpráva, kterou přijmeme při čtení pošty
- **Přílohy** – u této části e-mailu dochází k zakódování poštovním klientem před odesláním z důvodu snadnějšího čtení e-mailovými servery, které poštu odesílají, přijímají a předávají dále.

E-mailová hlavička, jak již bylo napsáno výše, obsahuje klíčové informace, které umožňují putování e-mailu do cíle neboli k adresátovi. Mezi tyto informace patří:

- **X-Originating-IP** … tato informace nám říká, z jaké IP adresy byl e-mail poslán
- **X-Originating-Email** … zde se jedná o e-mailovou adresu, ze které byl e-mail poslán
- **From** … tento řádek obsahuje adresu odesílatele, resp. jeho reálné jméno

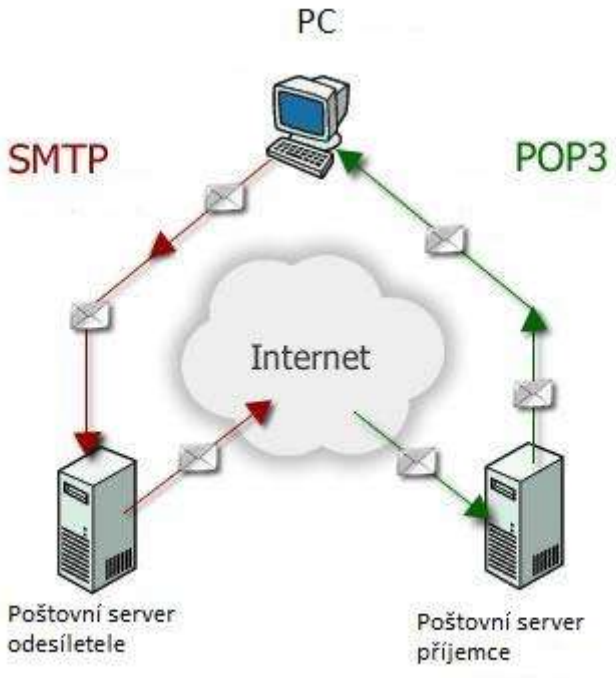
  * U těchto tří položek není zajištěna důvěryhodnost odesílatele, všechny položky mohou být změněny odesílatelem!
- **To** … zde se zadává adresa kam má být e-mail odeslán
- **Received** … do received je zaznamenána cesta e-mailu po jednotlivých serverech. Kdykoliv je e-mail předáván serverem dál, doplní se údaje o serveru, z nějž byla zpráva přijata, název serveru kterým byla přijata, čas jejího zpracování a jedinečný identifikátor. Díky těmto informacím mohou e-mailové servery filtrovat spam a informovat uživatele o tom co se s jeho zprávou dělo během její cesty.

- **Mime-Version** a **Content-Type** …tyto informace specifikují obsah e-mailu. Informují, zda se jedná o prostý text nebo zda je naformátován v HTML. Slouží k tomu, aby e-mailový klient zobrazil zprávu ve správném formátu. [XXV]

3.3.1. Protokoly elektronické pošty

Základní protokoly používané pro provozování e-mailových serverů jsou SMTP, POP3 a IMAP. V následující části se na tyto tři protokoly podíváme detailněji.

Obr. 2 – Protokoly SMTP a POP3



Zdroj: *vlastní*

3.3.1.1. SMTP

Simple Mail Transport Protocol (jednoduchý protokol přenosu pošty) je protokol používaný pro odesílání, předávání a přijímání e-mailů na příslušné servery. SMTP přijímá připojení na portu 25 a běží ve formě démonového procesu. Pravidla pro komunikaci mezi přenosovými složkami (poštovními servery) jsou dána dokumentem RFC 821 (*Requiest For Comment*). Komunikace mezi odesilatelem zprávy a příjemcem probíhá formou žádostí - příkazů

vznášených odesílatelem. SMTP zabezpečuje odeslání zprávy z klientského počítače na klientův server a dále na klientský server příjemce. [XXV]

3.3.1.2. POP3

Post Office Protocol 3 byl standardizován v roce 1993. Protokol POP3 zajišťuje přenos došlých zpráv z poštovní schránky uživatele na klientském serveru do klientského prostředí uživatele. Tento protokol běží na portu 110. Server POP3 vyžaduje po každém uživateli, aby měl svoje jméno a heslo. Tento protokol byl velice výhodný pro uživatele s omezeným přístupem k internetu, jelikož se připojí jen na dobu nezbytnou pro stažení zpráv a poté se opět odpojí. Zprávy se po stažení z daného serveru smažou, což může být výhoda pro uživatele, kteří dostávají velké množství pošty. Nicméně je zde samozřejmě možnost tyto zprávy na serveru ponechat. Pro zabezpečení lze použít SSL či TLS šifrování. [XXI]

3.3.1.3. IMAP

Internet Mail Access Protocol je také protokol pro připojení k serveru a převzetí e-mailu. Tento protokol je novější a zároveň i složitější než POP3. Mezi jeho další funkce kromě stahování zpráv patří vyhledávání ve zprávách, obousměrný přenos (tedy uložení na server - například u odeslané pošty), asynchronní notifikace (přijde zpráva a okamžitě se stáhne, bez čekání na periodickou kontrolu), práce se složkami, schránka může být otevřená z více počítačů současně, práce s přílohami (bez stahování celé zprávy), příznaky zpráv (např. přečtená, odpovězená...). Rovněž podporuje SSL a TLS šifrování. IMAP ale nemá na rozdíl od POP3 podporu u všech klientů. Díky protokolu IMAP serveru je možno přistupovat k poště přes webový prohlížeč a mít tak své zprávy k dispozici jak doma, tak třeba v práci. [X]

3.3.1.4. MIME

Multipurpose Internet Mail Extension je nadstavba SMTP. Podle původní koncepce elektronické pošty bylo možné přenášet zprávy pouze v anglickém jazyce, tzn. bez diakritiky či dalších mezinárodních znaků. Proto vznikl protokol MIME, který měl zajistit přenos 8bitových dat a určovat povahu netextových dat, aby příjemce dokázal rozpoznat netextová data. MIME zakóduje dopis podle RFC 822 na straně odesílatele a rozkóduje na straně příjemce. Pro protokol MIME je nutná podpora na straně odesílatele i příjemce. Jednotlivé typy jsou text, image, audio, video, application, message, multipart. [XXVII]

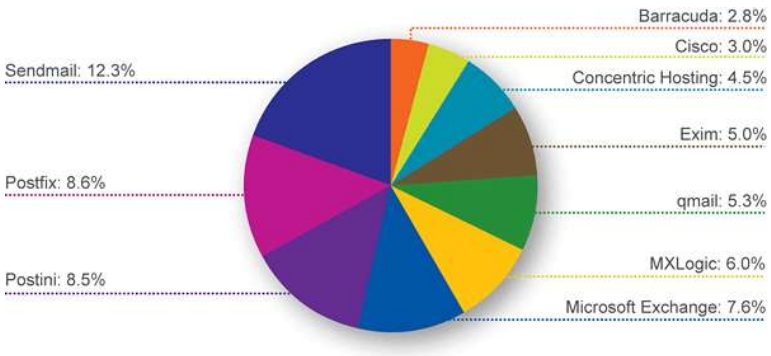
3.3.2. Agenti přenosu elektronické pošty

Mail Transfer Agent (MTA) je přenosový agent zajišťující správný formát zprávy a její odeslání směrem k adresátovi. Plní roli klienta (když má zprávu k odeslání) nebo serveru (pokud je vyzván jiným MTA k převzetí zprávy).

User Agent (UA) umožňuje přímé čtení doručených zpráv uložených v lokální poštovní schránce a také odeslání nově vytvořené zprávy na specifikovanou adresu.

Mail Delivery Agent (MDA) je doručovací agent, který ukládá zprávy do příslušných poštovních schránek jednotlivých uživatelů. [XXIV]

Obr. 3 – Podíl jednotlivých MTA v roce 2007



Zdroj *: http://www.oreillynet.com/lpt/a/6849 ,21.3.2009*

3.3.2.1. Sendmail

Vznikl v roce 1980 a stal se součástí systému 4.0 BSD. Dnes patří mezi nejrozšířenější agenta přenosu elektronické pošty. Mezi jím používané standardy patří podpora IPv6, smtp autorizace, blacklisty, filtry (nazývané milter). Sendmail je dnes často součástí již unixových systémů jako výchozí MTA, např. FreeBSD. Mezi jeho výhody určitě patří antivir (clamav) a antispam (spamassassin), které dokáží velmi účinně filtrovat poštu od nevyžádaných zpráv (spamů). Dále sendmail podporuje virtuální domény a je také zajištěna podpora více uživatelů. [XVII]

3.3.2.2. Exim

Tento agent byl vyvinut na univerzitě Cambridge, Velká Británie, pro použití na unixových systémech. Je volně dostupný za podmínek GNU. Má velmi podobné vlastnosti jako Sendmail, ale má i několik dalších plus, např. velmi flexibilní v možnostech přesměrovaní mailů a také má rozsáhlé možnosti pro kontrolu příchozí pošty. [VI]

3.3.2.3. Postfix

Postfix vznikl v roce 1998 jako open-source software, jeho autorem je Wietse Venema (programátor a fyzik zabývající se převážně bezpečností). Vývoj a podpora byla sponzorována společností IBM Research. Postfix je podle jeho autora silný v několika kategoriích. Je to hlavně bezpečnost (má několik obranných vrstev, princip nejmenších oprávnění, nepotřebné moduly lze deaktivovat), výkon (omezení počtu nových procesů, počet přístupů k systému souborů), flexibilita (jednotlivé část lze upravovat pomocí jednoduchých konfiguračních souborů), spolehlivost (při vysokém zatížení upozorní na nedostatek paměti či diskového prostoru). [VII]

3.4. Databázový server

Databáze z IT pohledu je obecně software spravující určitý balík dat a umožňující uživatelům tento balík měnit a spravovat. Zároveň slouží k jejich organizaci, třídění, prohledávání, seskupování a podobně.

3.4.1.MySQL

MySQL patří mezi relační databáze. Tyto databáze se vyznačují ukládáním dat do tabulek neboli skupin záznamů. Každý záznam v tabulce může mít určité vlastnosti. Tyto vlastnosti mohou mít také své vlastní vztažené tabulky – odtud pochází termín relační databáze. Každá z tabulek může být spojena s jakoukoliv jinou prostřednictvím klíčů. Klíč je jednoznačný identifikátor přiřazený každému záznamu v tabulce.

Díky tomu, že je MySQL volně šiřitelný software (GPL licence), má v současné době vysoký podíl na používaných databází. [XXXV]

Jedná se o výkonného databázového správce, který byl vytvořen švédskou společností MySQL AB. Jeho hlavními autory jsou Michael Widenius a David Axmark. Umožňující ukládat a přebírat data pomocí skriptovacího jazyka, kterým může být např. PHP. Díky

MySQL je možno rychle, výhodně a s minimálními náklady ukládat různé typy dat (logické operátory, text, čísla, obrázky, binární číslice a rozsáhlé binární objekty). MySQL je systém obsahující mnoho funkcí, patří mezi ně např. replikování dat, uzamykání tabulek, omezování dotazů, uživatelské účty, více databází, trvalá připojení, uložené procedury, spouště a pohledy. [XXV]

3.5. PHP

PHP původně nazýván Personal Home Page Tools byl vyvinut v roce 1994 jako jednoduchý nástroj, který se vkládal do HTML a byl určen pro vytváření dynamického obsahu webových stránek. Jak se PHP postupem času vyvíjel, dosáhl podoby velmi výkonného a obecně použitelného nástroje pro vývoj webu. Dokonce se z něj stal jeden z nejpoužívanějších rozšiřujících modulů pro Apache.

PHP je skriptovací jazyk, který je na jedné straně poměrně jednoduchý a na druhé straně velmi výkonný. PHP umožňuje velmi dobré serverem analyzované skriptování. (Aulds, 2000)

Od doby, kdy PHP spatřil světlo světa, vyšlo několik dalších verzí. V roce 1995 se spojil s programem Form Interpreter a vznikla verze PHP/FI 2.0 .Koncem roku 1998 byla uvedena verze PHP 3.0, která byla rychlejší a vybavenější než předchozí verze. Postupně vyšly verze 4.0 až po dnešní verzi 5.2[9]. Mezi základní výhody PHP patří jak již bylo řečeno jeho jednoduchost, podobná syntaxe jazyku C, podpora široké řady souvisejících technologií, formátů a standardů. Dále je to otevřený projekt s rozsáhlou podporou, snadno komunikuje s databázemi (MySQL, PostgreSQL,..), je multiplatformní a lze jej provozovat s většinou webových serverů a na většině operačních systémů. [XXXVI]

[9] 14.11.09

4. Bezpečnostní analýza

4.1. Obecně o bezpečnosti

Naprosto bezpečný systém neexistuje [10]

Téma týkající se bezpečnosti jsem začal citací, kterou ve své knize uvedl Pavel Satrapa [XXVII] (specializující se na počítačové sítě), z jednoho důvodu. Tímto důvod je, že zabezpečení je velmi široké a zároveň složité téma. Můžeme říct, že se podmínky mění téměř každý den. Je potřeba být neustále informován o současných trendech, novinkách či aktualizacích.

Webové servery se v minulosti staly mnohokrát terčem útoků za účelem změny obsahu, získání citlivých údajů a dat či poškození operačního softwaru nebo jiného programového vybavení. Základní rozdělení útočníků podle Krčmáře [XIV] je na průzkumníky a crackery. Tyto dvě skupiny jsou rozděleny nikoliv podle jejich schopností ale podle jejich záměru.

Za **průzkumníka** je považován uživatel, který nemá v úmyslu něco poškodit či zničit. Tento druh útočníků se snaží proniknout do systému, najít v něm chyby a dokázat si svoje schopnosti. Dokonce se dá tato činnost nazvat určitým druhem sportu, protože průzkumníci se sdružují často ve skupinách a soutěží mezi sebou, kdo dokáže překonat větší překážky v podobě zabezpečení systému. Hlavní jejich cíl je dostat se pokud možno všude.

Druhou skupinu tvoří **crackeři**. Tato skupina je mnohem nebezpečnější, protože crackeři si vybírají svoje „oběti“ cíleně a jejich hlavním cílem je zisk. Tento cíl může být finanční či se může jednat o získání dat za účelem jejich prodeje. Někteří mohou pracovat jako najmutí vyhledávači informací (plány nového produktu, seznam zákazníků, informace o bankovních účtech, atd.) či jako likvidátoři konkurence. Další skupinka crackerů se zabývá prolamováním ochrany komerčního softwaru, čímž způsobuje škodu majiteli autorských práv. Crackeři dokážou napáchat velmi vysoké škody. [XIV]

Na bezpečnost serveru se můžeme dívat z několika pohledů. Tím prvním je fyzické zajištění serveru. Tady se jedná hlavně o hardwarovou bezpečnost. Další pohledy jsou z hlediska síťově bezpečnosti. Tu můžeme rozdělit na lokální uživatele (s přístupem na daný počítač) a

[10] Satrapa, P., Randus, J.A. *Linux – Internet server*., Praha: Neokortex, 1996 413 s., ISBN 80-902230-0-1

externí uživatele (u Internetu). Satrapa [XXIX] tvrdí, že více jak 80% útoků je způsobeno lokálními uživateli. V následujících kapitolách si jednotlivé kategorie podrobněji rozvedeme.

4.2. Fyzické zajištění serveru

Jedná se o ochranu hardwaru a fyzické zabezpečení systémů, jako je přístup k jednotkám CD-ROM či DVD-ROM, dále flash diskům a dalším paměťovým modulům. Podle Krčmáře[XIX] by útočníkovi měl být znemožněn přístup k serveru, aby nemohl jakkoliv pozměnit software na něm nainstalovaný, např. pomocí jím přineseného datového media. Proto by první linií obrany měly být prostředky, které zabrání útočníkovi, aby se dostal k serveru. Pro skladování dat je velmi vhodné mít speciální vyhrazenou místnost s omezeným přístupem jen pro pověřené osoby. Pokud útočník překoná tuto překážku, dalším stupněm zabezpečení může být speciální skříň (např. s indikací otevření) chránící server, která dokáže upozornit administrátora na otevření či na pokus o otevření této skříně. Další prostředek obrany může být ponechání serveru bez jakýkoliv vnějších periferií jakými mohou být monitor, klávesnice či myš. Architektura serveru je vybavena pro vzdálený přístup, čímž nám odpadá přítomnost těchto periferií. Krčmář [XIX] dále upozorňuje na vedení kabelů a rozvodů, i když to se někdy ovlivnit nedá. Doporučuje všechny kabely chránit vhodnými lištami, rovněž switche a routery chránit pomocí speciálních skříní proti vnějšímu zásahu. V opačném případě mohou být volnou cestou do systému.

V předchozím odstavci jsem se zabýval nebezpečím z hlediska útoku vedeného člověkem. V tomto odstavci bych rád také zmínil určitá rizika v podobě fyzikálních jevů.

Prvním jevem je **elektřina**, která je nutná pro chod a provozování veškeré výpočetní techniky. A proto při výpadku napětí v elektrické síti může dojít k výpadku serveru či poničení počítačového zdroje a dalších zařízení. Krčmář [XIX] doporučuje mít dostatečně dimenzovaný zdroj záložního napájení (UPS), který dokáže zabezpečit chod i během výpadku napětí. V tomto případě je důležitá konektivita mezi počítačem a záložním zdrojem z důvodu poskytování informací o stavu baterií a sítě. Dále nutné zajistit, aby i další síťové komponenty (router, switch, atd.) zůstaly v provozu, protože běžící server bez připojení k síti je bohužel k ničemu. Navíc UPS dokáže zachytit a odfiltrovat výkyvy v elektrické síti a tím předejít poškození zařízení k němu připojené.

Dalším faktorem může být **teplota** a **vlhkost vzduchu.** Podle Krčmáře[XIX] bývá teplota velmi často podceňována. Počítače a další elektronika je sama o sobě velkým tepelným zdrojem. Proto je doporučeno místnost s počítači vhodně klimatizovat a udržovat přibližně stálou teplotu (kolem 20°C). Klimatizace rovněž dokáže řešit i problém vlhkosti, která by se měla pohybovat mezi dvaceti a třiceti procenty. Vysoká vlhkost může způsobit zkratování obvodů a při nízké vlhkosti vzniká statický náboj, který může probíjet mezi jednotlivými částmi počítače a ohrozit tak data. Problém může rovněž nastat při odvádění tepla z vnitřního prostoru počítače ven. Zde existuje mnoho řešení, mezi které patří např. přídavné větráky, pasivní chlazení či dokonce vodní chlazení. Velmi důležité je mít určité záložní řešení v případě selhání některé z části chladicího systému. Tímto řešením mohou být výkonné přídavné větráky, které se zapnou při detekci vyšší teploty než je standart.

Mezi další jevy patří **voda** a **oheň.** Na počátku 21. st. (hlavně v roce 2002) došlo v České Republice k velmi rozsáhlým záplavám, které způsobili nemalé škody i v oblasti výpočetní techniky. Došlo k zaplavení místností s počítači, servery, databankami. Po opadnutí vody byly všechny poškozené počítače odvezeny rovnou k likvidaci. Proti tomuto živlu je možno se chránit vhodným umístění výpočetní techniky mimo problematické oblasti popř. umístěním do vyšších pater budov. Dalším „vodním“ problémem mohou být vodovodní rozvody. Umístění serverovny pod hlavní rozvod vody může způsobit opět velké škody v případě havárie tohoto vedení. Rovněž oheň může způsobit velké škody na technice. Zde je doporučován automatizovaný protipožární systém a navíc mít při vchodu do místnosti s výpočetní technikou hasicí přístroj (práškový, ne vodní ani s CO_2). [XIX]

Hlavním bodem, který jsem se snažil zdůraznit, je prevence. Investice, které nám pomůžou ochránit náš systém, jsou mnohem nižší než škoda způsobená nedostatečným zajištěním. Ztráty způsobené výpadkem mohou mít pro firmu či společnost fatální dopady hlavně v podobě ztráty dat.

4.3. Počítačová síť a její bezpečnost

Počítačová síť je podle Vychodila [XXXIV] systém propojující jednotlivé hostitelské počítače. Po propojení hostitelských počítačů je možné sdílet data a vzájemně využívat nabízených služeb popř. technických prostředků (drahé periferie, kapacity disků, atd.). Mezi další výhody sítě patří vzájemná komunikace umožňující posílat elektronickou poštu, komunikaci mezi

programy (např. distribuované aplikace). Síť rovněž umožňuje díky propojení počítačů zálohování dat na více místech pro případ výpadku.

4.3.1. Druhy síťových útoků

Podle Krčmáře [XIX] se dají síťové útoky rozdělit do několika skupin či oblastí. Tou první je **útok na webový server.** Takový útok je nejčastěji proveden díky nějaké chybě či mezeře v PHP skriptu či CGI skriptu. Chyba nastává při neošetření vstupů a díky nim může útočník předávat příkazy a měnit obsah databáze. Často se také stává, že mnoho webmasterů ukládá svoje hesla v otevřené podobě do skriptů. Což je sice pohodlné, ale zároveň velmi nebezpečné.

Dalším útokem je **odposlech komunikace.** V tomto případě se jedná o odposlechnutí dat (čtení TCP paketů), která se pohybují po internetu či lokálních sítí bez zašifrování. Mezi služby, které jsou takto ohroženy, patří např. FTP, HTTP, telnet, POP3, SMTP, atd. Vhodným prostředkem pro prevenci odposlechnutí slouží SSH server, který posílá data šifrovaným kanálem či tunelem. Popřípadě lze použít systém certifikátů a zajistit, aby data četl jen, ten komu jsou určena.

Denial of service (DoS) je útok, který spočívá v zahlcení serveru daty. Jakmile se server zahltí, nedokáže již dále pracovat a zkolabuje. Tomuto útoku se odolává velmi špatně. K útoku se často používají vadné pakety, nesmyslné dotazy nebo otevírání spojení, které nejsou uzavírána. Obranou proti takovému útoku může být kontrola počtu připojení z jedné IP adresy a při překročení určitého počtu spojení dojde k zakázání dalších příchozích z této adresy. DoS se dělí na několik druhů. Prvním jsou *reflektivní útoky*, které spočívají v zahlcení linky oběti a využívající k útoku jiné počítače či routery jako prostředníky. Při takovém útoku je velmi těžké vypátrat útočníka, neboť útok se odráží od dalších počítačů a serverů. Jedním z nejvíce nebezpečných útoků je DNS zesilující útok. Tento útok spočívá v posílání DNS dotazů a může dosáhnout až 70 násobku původních dat. Mezi další typ DoS patří *záplavové typy útoků*. Tento útok spočívá ve vygenerování co největšího toku, aby zahltil linku oběti. Velmi záleží na rychlosti připojení k internetu ale i servery, které jsou připojeny velmi rychlou linkou, mohou být zahlceny a to díky DDos (data posílají stovky či tisíce počítačů). Mezi DoS útoky také patří *útoky využívající chyb*. Útočník se v tomto případě soustředí na software, který obsahuje nějaké chyby. Jinými slovy, útočník si dokazuje, že je lepší než ten, kdo software vytvořil, popř. ho provozuje.

Jsou i další druhy útoků, např. **podvržená IP adresa**. Některé firewally propouští pakety pouze z předem definovaných IP adres, ale může se stát, že útočník dokáže svojí IP i MAC adresu změnit a pak už mu nic nebrání posílat pakety, které by normálně neprošly. Ověřování IP adresy jako jediný způsob ověření totožnosti není nejlepší řešení z pohledu bezpečnosti.

4.3.2. Protokoly TCP/IP

Jedná se o ucelenou síťovou koncepci, která může být použita v jakékoli počítačové síti, a to jak lokální, tak i rozlehlé. Součástí této koncepce je dnes více než 100 různých konkrétních protokolů, a další neustále vznikají.

TCP/IP neboli **Transmission Control Protocol / Internet Protocol** je hlavní komunikační protokol sítě Internet a nejenom jí. Původně sloužil jako protokol v síti ARPANET (předchůdce sítě Internet, fungovala od roku 1969 do roku 1989-90), kde nahradil původní protokol NCP. Architektura TCP/IP je složena ze čtyř vrstev hierarchicky uspořádaných. Mezi tyto vrstvy patří síťová vrstva, transportní vrstva, aplikační vrstva a vrstva síťového rozhraní. [XXXIV]

Tab. 2 - Vrstvy TCP/IP

Aplikační vrstva	Aplikační protokoly (FTP, TFTP, HTTP, HTTPS, TELNET, POP3, SMTP, IMAP, RPC, DHCP, DNS, NTP, atd.)
Transportní vrstva	TCP, UDP
Síťová vrstva	IP, ICMP, ARP, RARP, SLIP, PPP
Vrstva síťového rozhraní	Ethernet, Token Ring, ATM, FDDI, HDLC

Zdroj*: vlastní*

4.3.2.1. Aplikační vrstva

Aplikační vrstva je nejvyšší vrstva síťové architektury TCP/IP a je tvořena jednotlivými službami, které jsou definovány vlastními protokoly. Ty to protokoly se dají rozdělit na dvě skupiny, pro administrativní a uživatelské aplikace.

- Protokol HTTP (HyperText Transfer Protocol)

Tento protokol definuje pravidla komunikace mezi serverem a klientem, a tvoří základ WWW. Většina stránek je přepravována pomocí tohoto protokolu. HTTP je bezstavový protokol, což znamená, že si server neudržuje žádné informace o svých klientech. Z pohledu HTTP to znamená, že v případě obdržení dotazu na něj odpoví a tím skončí ucelená transakce.

Stavové informace si pamatuje klient. Celá transakce probíhá následovně. Uživatel dá pokyn (dotaz), např. výběrem odkazu na stránce. Potom klient určí URL informace, které má získat (dozví se který protokol použít, jaký server kontaktovat, co po něm chtít). Následně klient naváže transportní spojení se serverem a pomocí tohoto spojení odešle dotaz. Server tento dotaz zpracuje a odešle odpověď. Tím celá transakce končí a spojení se uzavře.

Protokol HTTP prošel poměrně značným vývojem během své existence. První verze byla 0.9 a dovolila pouze přenos dat ze serveru ke klientovi. Potom ji nahradila verze 1.0 (definovaná jako RFC 1945). Tato verze přinesla oproti předchozí možnost doplnit spojení o řadu dalších informací (např. typ dokumentu, jeho vznik, požadavky klienta,atd). Dnes patří mezi standard verze 1.1 definovaná jako RFC 2616. [XXVIII]

- Protokol FTP (File Transfer Protocol)

Tento protokol je jedním z nejstarších aplikačních protokolů a slouží k přenosu souborů mezi uzly připojenými k Internetu. Mezi základní vlastnosti FTP patří interaktivní přístup (většina implementací poskytuje uživatelské rozhraní pro interaktivní práci se vzdálenými servery), specifikace formátu (klient může specifikovat typ a formát uložení dat – binární, textový ASCII nebo EBCDIC, apod.) a řízení přístupu (přihlašovací procedura pomocí jména a hesla, přenášeny v nezašifrované podobě).

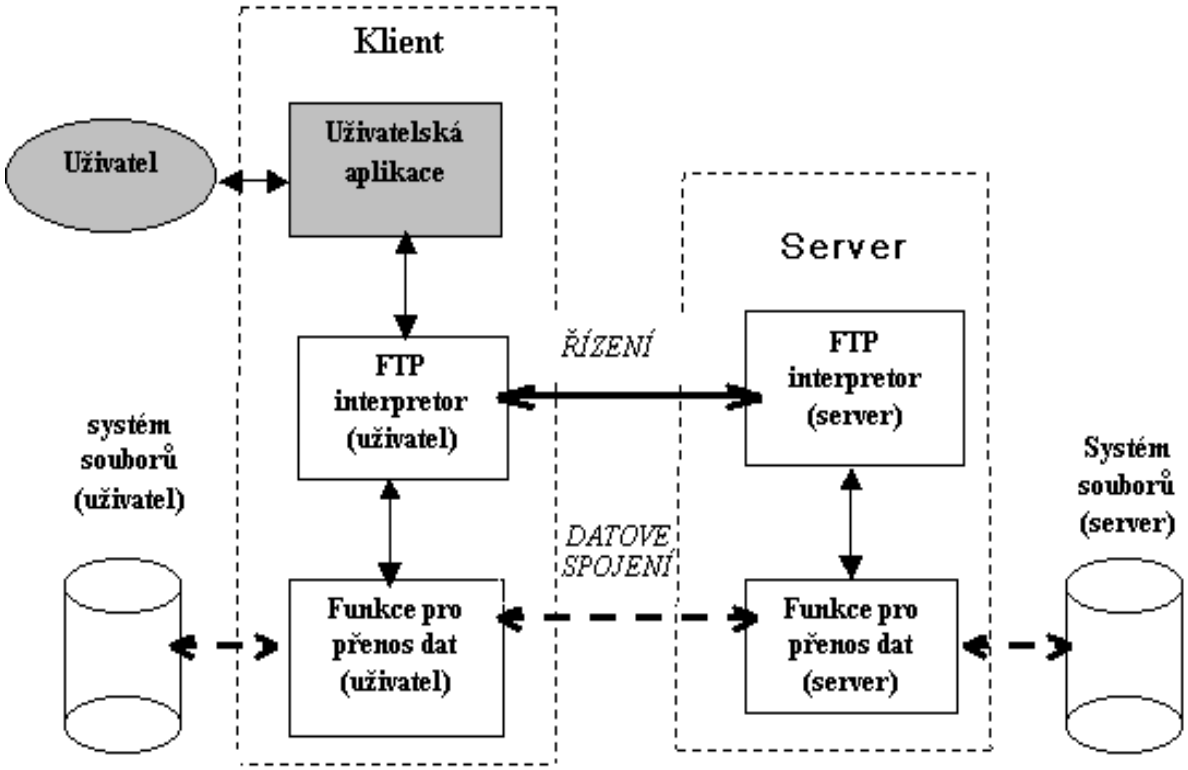
Relace protokolu FTP je typu klient-server (viz. Obr. 4). Klient, uživatel služby, pracuje s programem ftp umožňující mu navázat relaci se zvoleným serverem, zadávat mu své požadavky a relaci uzavřít. Na serveru (poskytoval služby) běží program, který po oslovení klientským programem ověří jeho oprávnění k přístupu do svého souborového systému a poté, až do ukončení relace, plní klientovy příkazy.

FTP používá dvě spojení, řídící a datové. Řídící spojení (běží na portu 21) běží po celou dobu relace a přenáší se po něm příkazy a odpovědi mezi klientem a serverem. Datové spojení (běží na portu 20) je určeno pouze pro konkrétní přenos dat a slouží tak pro přenos vyžádaných dat.

FTP klient se musí v rámci řídícího spojení autentizovat a to pomocí jména a hesla. Existují ale i anonymní FTP servery, které umožňují veřejný přístup k části svého souborového systému. Většinou jsou na těchto serverech k dispozici volně šiřitelné programy, ale také obrazový materiál, manuály, obsahy časopisů, apod.

Z pohledu bezpečnosti nebyl samotný přenos souborů dobře zabezpečen, proto se používaly další metody jak zvýšit bezpečnost přenosu, např. zašifrování souboru před samotným přenosem. Později byl protokol rozšířen o lepší zajištění autenticity a autorizace uživatelů. [XXIV]

Obr. 4 - Komunikace protokolu FTP



Zdroj:*[XXIV], str. 408*

- Protokol Telnet

Telnet je protokol pro vzdálený přístup. Umožňuje přihlášení ze vzdáleného počítače na jiný počítač a následně interaktivní práci na něm. Uživatel díky telnetu může využít svůj hardware a vzdálený software, popř. i vzdálené periferie. Aby mohl uživatel takto pracovat je nutná podpora protokolu telnet na obou počítačích. Dále musí mít uživatel patřičná oprávnění pro využívání vzdáleného zařízení. Je zde nutná z důvodu ochrany autentizace uživatele pomocí jména a hesla.

Telnet standardně běží na portu č. 23. Protokol Telnet zahrnuje dva aplikační programy. První je Telnet klient, který vytváří komunikační rozhraní a používá příkazový řádek, převádějící jednotlivé znaky skutečného terminálu do formátu pro přenos. Druhý aplikační program je

Telnet server, který je spuštěný na vzdáleném uzlu. Je to prostředník mezi vzdáleným terminálem a programy a utilitami lokálního systému.

Mezi vlastnosti telnetu patří tři základní prvky: definuje síťový virtuální terminál (poskytuje jednotné standardní rozhraní pro přístup ke vzdáleným systémům), volitelnost režimů (umožňuje klientovi a serveru vzájemné rovnocenné vyjednávání z určité předdefinované množiny), spojení považuje za symetrické (klientem může být jakýkoliv proces, nerozlišuje mezi terminály a procesy). [XXIV]

4.3.2.2. Transportní vrstva

Hlavním úkolem této vrstvy je zajistit přenos mezi dvěma koncovými účastníky, kterými jsou v případě TCP/IP přímo aplikační programy (jako entity bezprostředně vyšší vrstvy). Podle jejich nároků a požadavků může transportní vrstva regulovat tok dat oběma směry, zajišťovat spolehlivost přenosu, a také měnit nespojovaný charakter přenosu (v síťové vrstvě) na spojovaný. Nabízí transportní službu se spojením nebo bez spojení za použití jednoho ze dvou protokolů:

- TCP (Transmission Control Protocol) – poskytuje transportní službu se spojením, včetně řízení koncového zabezpečení a datového toku, jedná se o spolehlivý transportní protokol – díky tomu je využíván aplikačními službami jako např. FTP či Telnet. Pro aplikační vrstvu TCP poskytuje službu plného duplexu (data je možno posílat v obou směrech nezávisle na sobě).
- UDP (User Datagram Protocol) – poskytuje jednoduchou transportní službu bez spojení, jedná se o nespolehlivý transportní protokol. Aplikace, které tento protokol využívají, nepožadují zabezpečení přenosu v takovém rozsahu, jaký nabízí TCP nebo pro transakčně orientované aplikace.

4.3.2.3. Síťová vrstva

Tato vrstva je také někdy nazývána jako vrstva internetu. Její funkce jsou síťová (logická) adresace, směrování a předávání datagramů přes komunikační podsíť, včetně směrování. Mezi další funkce patří segmentace a znovusestavování datagramů do a z rámců specifikovaných protokolem nižší vrstvy. Protokoly, pracující v této vrstvě, poskytují následující síťové služby:

Segmentace, sestavování a předávání datagramů (paketů)

- Protokol internetu (IP, Internet Protocol) – poskytuje síťovou službu bez spojení a zodpovídá za vysílání datagramů na základě síťových adres obsažených v jejích záhlavích. IP nezaručuje doručení datagramu, je proto tato síťová služba nazývána jako nespolehlivá. Architektura TCP/IP se spoléhá na protokoly vyšších vrstev (zajištění opětovného přenosu v případě ztráty datagramu), protože nepoužívá na síťové úrovni žádné spolehlivé protokoly. V současné době se používají dvě verze protokolu, IPv4 a IPv6.

Mapování adres

- Protokol mapování adres (ARP, Address Resolution Protocol) – používá se při znalosti cílové IP adresy stanice (rozhraní) pro nalezení příslušné fyzické adresy rozhraní (MAC).
- Protokol obráceného mapování adres (RARP, Reverse Address Resolution Protocol) – používá se při znalosti vlastní fyzické adresy pro získání vlastní IP adresy při zahájení práce (např. v případě bezdiskových stanic)

Řízení

- Protokol řídících hlášení (ICMP, Internet Control Message Protocol) – slouží k přenosu specifických zpráv týkající se chyb a zvláštních okolností při přenosu datagramů

Směrování

- Směrovací protokoly (OSPF, Open Shortest Path First; IGRP, Interior Gateway Routing Protocol; E-IGRP, Enhanced Interior Gateway Routing Protocol)
- Protokol virtuálního směrovače pro zálohování (VRRP, Virtual Router Redundancy Protocol)
- HSRP (Hot Standby Router Protocol)

Správa skupin stanic

- Protokol správy skupin (IGMP, Internet Group Management Protocol)

4.3.2.4. Vrstva síťového rozhraní

Je to nejnižší vrstva architektury TCP/IP, která umožňuje přístup k fyzickému přenosovému médiu. Je přímo zodpovědná za přístup k síti, a proto je specifická pro každou síť podle její implementace. Protokoly této vrstvy doručují data jiným systémům připojeným do sítě. Toto rozhranní musí znát, na rozdíl od ostatních vrstev, detaily konkrétní síťové infrastruktury (adresaci, formáty dat. jednotek, atd.) ,aby se mohlo provést správné formátování do rámců podle daných omezení. V současné době se může využívat všech známých typů přenosových prostředí, lokálních sítí (Ethernet, Token Ring, FDDI) i rozlehlých sítí (X. 25, ATM) pro podporu TCP/IP. Mezi hlavní úkoly této vrstvy patří zapouzdřit datagramy IP do rámců odpovídajících formátů a délek pro přenos daným rozhraním, dále je zodpovědná za mapování síťových adres na adresy fyzické používané na spojové vrstvě (adresy MAC).

4.3.3.Řízení přístupu

Zahrnuje omezení založená například na aktuálním čase, IP adrese či doméně klienta, typu šifrování datového přenosu, počtu přihlášení či dotazů uživatele za poslední den apod. Podle Brůhy (2008) existují tři hlavní směry řízení přístupu:

- Volné řízení přístupu – DAC – Discretionary Access Control

Odvozuje se od identity uživatele nebo jeho členství v některé uživatelské skupině, tedy na základě autentizačních údajů, které uživatel předtím poskytl a pravidel, která každému uživateli a objektu v systému přiřazují typ povoleného přístupu. Tento volný přístup je charakterizován plnou kontrolou uživatele nad svými procesy a souboru. Rovněž může tento uživatel poskytnout některá práva jiným uživatelům k přístupu k těmto souborům a také udělují druh přístupu (čtení, zápis, kopírování, atd.).

- Povinné řízení přístupu – MAC – Mandatory Access Control

U tohoto přístupu jsou práva přístupu definována administrátorem a nemohou být změněna jiným uživatel jako tomu je u DAC. Objekty, uživatelé a procesy jsou hierarchicky seřazeny. Tato hierarchie zajišťuje, aby se informace klasifikované na vyšších úrovních nedostávaly k dispozici uživatelům, kteří neodpovídají svým zařazením této úrovni. A zároveň není povoleno uživatelům zapisovat do objektů s nižším stupněm klasifikace (vyloučení úniku informací do nižších úrovní). Tento systém tak má vyhovět organizacím, které požadují vysoké zabezpečení (vojenské a vládní organizace, popř. i komerční organizace)

- Řízení přístupu založené na úrovních citlivosti – RBAC – Role Based Access Control

Tento přístup je založen na rolích a odpovědnostech každého uživatele v rámci organizace nebo uživatelské základny. Administrátor rozhoduje o přidělení rolí. Tento systém by měl být založen na zásadě co nejmenších oprávnění. To znamená, že každý uživatel má přístup jen k těm aplikacím a souborům, které skutečně potřebuje nikoliv k těm, které by mohl potenciálně využít. [III]

4.3.3.1. Autentizace

Autentizace je proces, při kterém se ověřuje a potvrzuje totožnost uživatelů. Při tomto procesu můžeme zjistit jednoznačnou identifikace (zjištění identity uživatele) nebo verifikaci uživatele (potvrzení identity uživatele) na základě zadaných údajů do databáze popř. autentizačního systému.

Zde jsou tři možné způsoby, jak lze ověřit totožnost uživatele, které jsou využívány pro kontrolu oprávnění přístupu k síti a ověření jejich práv vykonávat určité úkony, podle toho:

- **kdo jsou** – identifikace podle jednoznačných ukazatelů – biometrické znaky (DNA, otisk prstu, vzor oční duhovky, vzor oční sítnice, geometrie ruky, verifikace hlasu, atd.). Velkou výhodou těchto znaků je jejich nesnadná zaměnitelnost, ale na druhou stranu zařízení schopná takto identifikovat uživatele jsou velmi nákladná.
- **co mají** – identifikace podle vlastnictví určitých předmětů (čipové karty, osobní identifikační karty, klíče, atd.). Mezi výhody patří jednodušší možnost ověření autorizace, ale hrozí riziko ztráty, kopie, krádeže. V případě ztráty či krádeže hrozí ztráta dat či peněžních prostředků. Tyto prostředky identifikace se také nazývají tokeny (memory tokens či smart tokens). Mezi nejčastější prvky patří čipové karty, které obsahují informace k ověření identity uživatele. Karta vyžaduje speciální čtecí zařízení na straně autentizující subjektu a navíc heslo (PIN), které zvyšuje její odolnost vůči narušitelům.
- **co znají** – identifikace pomocí přístupových hesel, číselných kombinací, osobních identifikačních čísel, atd. Je to nejjednodušší způsob zabezpečení. Ale hrozí tu riziko zapomenutí, zneužití v případě jejich záznamu na jakémkoliv mediu, vyžadují určité specifikace proti uhádnutí (přítomnost čísel, nealfanumerických znaků, velkých a malých písmen, nesmí se jednat o slovo ze slovníku) a pravidelnou obměnu. Tím se samozřejmě zvyšuje riziko jejich zapomenutí.

Autentizace může probíhat jednosměrně, kdy probíhá autentizace pouze jedné strany vůči druhé nebo obousměrně, kdy dochází k autentizaci obou stran a dochází ke sdílení určité tajné informace. Tento způsob může být časem obtížnější z hlediska tvorby, ukládání a přenosu těchto informací. Proto se častěji využívá autentizace za pomoci třetí důvěryhodné strany (využívá symetrické šifrování a šifrování veřejným klíčem). [XXIV]

4.3.3.2. Autorizace a účtování

Autorizace určuje, jaké operace mohou uživatelé v systému provádět a jaká data jsou pro ně dostupná. Je plně závislá na autentizaci, protože je tu předpoklad úspěšné autentizace a zařazení uživatele do uživatelských skupin či přístupových seznamů.

4.3.4.Šifrování a bezpečnost elektronické pošty

Základním kamenem úrazu je bezpečný přenos dat, aby se obsah zprávy dostal pouze k jejímu příjemci. Běžný přenos dat po Internetu je zcela nezabezpečený a data jsou přenášeny otevřeně, což znamená, že je může přečíst i kdokoliv jiný než adresát. Pro zabezpečení elektronické pošty slouží elektronický podpis a šifrování obsahu zprávy. Při vytváření bezpečné zprávy se používá asymetrická kryptografie. Ta pracuje s veřejným a privátním klíčem. Veřejný klíč data zašifruje a privátní potom slouží k dešifrování. Pouze držitel privátního klíče je schopen dešifrovat danou zprávu. Základním algoritmem pro šifrování je RSA a DSA (pro elektronický podpis). Zašifrování zprávy tedy řeší, aby její obsah byl znám pouze odesílateli a adresátovi. Elektronický podpis slouží k jasné identifikaci odesílatele. Bezpečnost elektronické pošty je tedy závislá na ochraně privátního a veřejného klíče. Tato ochrana spočívá hlavně v předejití narušení ochrany privátního klíče (disponuje s ním pouze jeho držitel), dále nesmí být prolomena šifrovací a hashovací funkce a v neposlední řadě musí být zaručena a ověřena autenticita veřejného klíče (klíč musí patřit dané osobě). [XV]

4.3.5.SSL a bezpečnost protokolů

SSL neboli Secure socket layer byl vyvinut v roce 1996 společností Netscape, který sloužil jak pro soukromé tak komerční účely. SSL je vrstva, která zabezpečuje data mezi aplikační a transportní vrstvou. Tato vrstva zajišťuje šifrování přenášených dat a autentizaci serveru díky digitálním certifikátům.

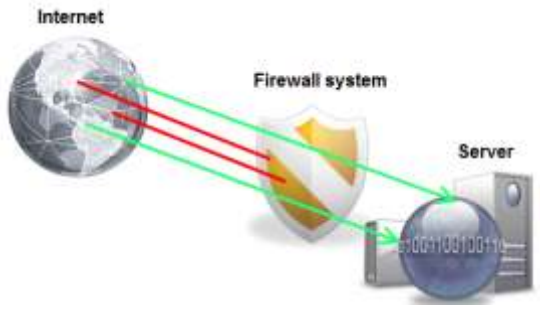
SSL je využíváno pro různé protokoly, např. je hojně využíván pro HTTP, FTP, SMTP, POP3, IMAP4, atd. Pokud protokoly využívají SSL, jsou doplněny o písmeno „s“ (HTTPS). Pro bezproblémový provoz SSL je nutná podpora na straně serveru i na straně klienta.

Autentizace probíhá, jak už bylo řečeno, pomocí digitálních certifikátů a je ověřována pravost klienta a serveru, s nímž jsme navázali komunikaci. Je používáno asymetrické šifrování s algoritmem RSA (digest a certifikáty). Digest je funkcí, která se snaží ztížit vytvoření funkce k ní inverzní a pro různé zprávy vracení různých digest. Certifikát je vydáván certifikační autoritou, která jej podepisuje svým soukromým klíčem a kdokoliv si pak může ověřit pomocí veřejného klíče dané certifikační autority jeho pravost.

4.3.6.Firewall

Firewall je prvek, který zvětšuje bezpečnost vytvářením určité hradby mezi serverem a Internetem, případně mezi lokální sítí a Internetem. Může se jednat o softwarový či hardwarový prvek nebo kombinaci obou. Firewall má na starost bezpečnou komunikaci mezi bráněným prvkem a veřejnou sítí. Firewall funguje na principu předem definovaných pravidel pro probíhající komunikaci a na základě těchto pravidel firewall filtruje příchozí a odchozí komunikaci, popř. některé služby rovnou zakáže. [II]

Obr. 5 - Firewall



Zdroj*: vlastní*

Firewall také monitoruje veškeré pokusy o průnik do sítě či nepovolené komunikace. Z protokolu firewallu je možné zjistit, zda se někdo pokouší o průnik, popř. kdy se pokusil, z jaké IP adresy a přes jaký port. Je třeba ale odfiltrovat zda se jedná o skutečný útok či jen chybu nebo omyl. Firewall lze nastavit dvěma způsoby, jako aktivní či pasivní. V případě pasivního nastavení pouze zapisuje podezřelé události do protokolu, zatímco aktivní při detekci nepovoleného rámce ho vyřadí. [V]

5. Analýza technického řešení včetně ekonomických aspektů

V této kapitole bych se chtěl zabývat HW nároky na server s přihlédnutím k ekonomické stránce provozování serveru. V prvé řadě bych se chtěl zmínit o možnosti VPS, znamenající virtuální privátní server bez nutnosti kupovat vlastní hardware. Virtuální server je vyhrazený prostor fyzického serveru, na kterém současně běží několik, zcela oddělených, virtuálních serverů.

Hlavním bodem této kapitoly je zjistit, jestli je z ekonomického hlediska výhodnější si server zakoupit anebo zda si jej pronajmout formou VPS. Taky bych chtěl udělat kalkulaci, ve které bude na jedné straně pronájem serveru a na druhé straně koupě serveru, platba za energii a další výdaje spojené s provozováním vlastního serveru.

V Tab. 3 jsou ceny pronájmu virtuálních serverů. Jako příklad jsem si vybral ceny od společností Fereng.cz(šedá barva) a FinalTek.com(modrá barva) neboť při procházení internetových nabídek společností provozující VPS jsem zjistil, že cenová nabídka je velmi podobná až na drobné rozdíly jak je vidět v tabulce níže. Můžete dostat rychlejší procesor, ale menší velikost HDD a podobně.

Tab. 3 – Ceny pronájmu VPS

Měsíční cena (Kč)	180	240	240	320	480	480	640	960	960	1280
CPU (MHz)	200	300	400	400	600	800	800	1200	1400	1600
RAM (MB)	128	192	192	256	384	256	512	768	512	1024
HDD (GB)	1	9	5	12	18	12	24	36	25	48

Zdroj: *http://www.vserver-hosting.cz/tarify-vps , 19.10.2009, Fereng.cz*
http://www.v-server.cz/cz/tarify/zobrazit/3, 19.10.2009, FinalTek.com

Při zjišťování hardwarové konfigurace vhodné pro webový server jsem oslovil dvě společnosti, iiCat zabývající se prodejem serverů od společnosti IBM a SWS a.s., zabývající se prodejem počítačových komponentů a softwaru. V závislosti na vytíženosti serveru, byla

vytvořena minimální a doporučená konfigurace serveru s operačním systémem Linux a webovým serverem Apache. Ceny, které jsou zde uvedeny odpovídají velkoobchodním cenám ze dne 19.10.2009 od daných společností (iiCat a SWS).

Tab. 4 – konfigurace serveru

	Minimální konfigurace	Doporučená konfigurace
Procesor	Intel Core 2 Duo E2200 2.20GHz/800MHz-1MB	Intel Xeon 3360 2.83GHz/1333MHz-12MB
Op.paměť	1GB PC2-5300 DDR2	8GB (4x 2GB) PC2-6400 CL6 ECC DDR2
HDD	73GB 15k RPM Hot-Swap SAS	146GB 15k RPM Hot-Swap SAS
Mechanika	DVD Multiburner	DVD Multiburner
HDD2	500GB 7.2k RPM SATA	1TB 7.2k RPM SATA
	22 876,-	43 380,-
UPS	Smart-UPS 750VA (500W) 5 830,-	
V obou případech se jedná o TOWER řešení	 server od spol. IBM	

Zdroj: *iiCat, SWS a.s., 19.10.2009*

Nyní můžeme provést celkovou kalkulaci, která varianta bude z dlouhodobého hlediska ekonomičtější-koupě serveru nebo jeho pronájem. Ještě bych chtěl upozornit na několik faktorů, které by mohly ovlivnit cenu vlastního serveru. Jedná se v prvé řadě o pronájem prostor, kde bude server umístěn. V případě vlastních prostor tento problém neřešíme a není zahrnutý ani v mé kalkulaci. Dále není kalkulováno s případnou koupí racku či nějakého jiného boxu pro ochranu serveru. Není započítaná drobná kabeláž či zásuvky.

Tab. 5 - Kalkulace

Pronájem		Koupě	
Měsíční paušál	1280,-	Server	22 876,-
		UPS	5 830,-
		Energie (400W zdroj, denní spotřeba 9,6kWh), cena za rok (ČEZ)	15 704,-
Cena pro 5-ti leté období	76 800,-	Cena pro 5-ti leté období	107 226,-

Zdroj:*vlastní, Veškeré ceny kalkulovány k 19.10.2009*

Z výše uvedených čísel nám lépe vyznívá varianta pronájmu serveru. Zde ale můžeme narazit na překážku v podobě webového prostoru a také výkonu serveru, který je nabízen.

Společnosti jsou schopné poskytnout v nejdražším pronájmu 48GB a konfiguraci, která se pouze blíží naší minimální konfiguraci. V případě vlastního serveru jsme limitováni počtem slotů pro HDD, tedy úložištěm dat. Ale ani to není neřešitelný problém, neboť pro ukládání dat se dají použít externí či síťové disky. Pokud bychom využili server uložený v racku, dají se aplikovat jako úložiště dat disková pole typu RAID.

6. Návrh webhostingové aplikace

Tato kapitola se bude zabývat konkrétní instalací všech prvků nezbytných k provozování webhostingu a zároveň zde bude nastíněno několik podkapitol, které by měly otestovat kvalitu a provedení dané aplikace.

6.1. Instalace jednotlivých prvků řešení LAMP

Jádro celého systému funguje na OS Linux, s konkrétní distribucí Ubuntu 9.10 pro serverové řešení. Popisovat celou instalaci Linuxu by nemělo smysl, proto se jen zmíním o některých bodech. Při zavádění Linuxu nám Ubuntu nabídne již připravenou verzi řešení LAMP. Já jsem ovšem tuto cestu nezvolil, a nainstaloval jsem jednotlivé prvky zvlášť. Při instalaci jsem pouze přidal balíček v podobě SSH serveru, který poskytuje zabezpečený komunikační protokol pro přenos dat přes nedůvěryhodnou síť, kterou bezesporu internet je.

Po dokončení instalace jsem pokračoval instalací dalších prvků - instalaci je nutné provádět jako administrátor v bashi (administrátorská práva získáme pomocí příkazu *sudo su*). Bash je unixový příkazový shell interpreter, který jsem využíval pro veškeré úpravy či instalací jednotlivých prvků webhostingového řešení. Další službu, kterou jsem nainstaloval a která bude běžet na mém serveru je DNS server v podobě BIND9. Získal jsem jej příkazem *aptitude install bind9* ,kde aptitude install je příkaz, který získá programy z dostupných zdrojů přímo pro konkrétní distribuci Linuxu. Opět pomocí příkazu aptitude install jsem také přidal balíček databázového serveru v podobě MySQL konkrétně ve verzi 5.0. Dalším prvkem byl emailový klient zastoupený službou Postfix (test funkčnosti je k dispozici v příloze). Pro chod emailové služby jsem také musel nainstalovat Courier IMAP a Courier POP3 server pracujících na portech 993, respektive 995 pro POP3. Obě služby jsou zabezpečeny pomocí SSL sloužící k šifrování komunikace mezi serverem a klientem. Jako předposlední službu jsem nainstaloval ftp server, který mi poskytl program proftpd. Nakonec jsem již přešel k instalaci webového serveru Apache verze 2.2 s jeho moduly PHP 5.2.6, Python, Ruby a WebDAV. Apache je již po instalaci plně konfigurován pro ostrý provoz a není potřeba dalších větších zásahů do jeho konfigurace. Apache je možné konfigurovat pomocí několika textových souborů, např. *apache2.conf*, *ports.conf* či *http.conf*.

Samostatnou kapitolu celé instalace tvoří služba ISPConfig. Více o celém programu je napsáno v kapitole 6.2. ‚teď bych zmínil pouze o instalaci tohoto softwaru. ISPConfig podporuje širokou škálu linuxových distribucí (Debian, Fedora, Mandriva, Ubuntu, SuSE, atd.) a umí spravovat všechny prvky webhostingového řešení, a proto je nutné mít všechny tyto prvky již nainstalované na daném stroji, než zahájíme vlastní instalaci ISPConfigu. Během instalace jsme dotázáni na několik otázek, některé z nich jsem dal do přílohy. Po dokončení instalace je ISPConfig přístupný na portu 81 a je nutné provést několik dalších kroků pro jeho bezproblémový chod. Je nezbytné uvést do chodu antispamový software v podobě open-source produktu SpamAssassin. Tento software dosahuje úspěšnosti filtrace 90-95%[11] a při detailnějším nastavení vzhledem k charakteristice konkrétního uživatele i vyšší. Poté je ještě nutné doinstalovat a nastavit Linux Quota.

6.2. Správa webhostingu - ISPConfig

Jako řešení správy webhostingu jsem použil komplexní řešení v podobě aplikace ISPConfig. Tato aplikace je velmi vhodnou pro správu neboť řeší web servery, FTP servery, databázové servery, DNS servery, uživatelské účty, emailové služby, zabezpečené přístupy (SSL), konfiguraci firewallů, antivirových programů a mnoho dalších služeb souvisejících s webhostingovou aplikací a její správou. ISPConfig je poskytován pod BSD licencí jako open source software.

Nyní se podíváme blíže na konfiguraci mé webhostingové aplikace pomocí ISPConfigu. ISPConfig využívá webové rozhraní a je dostupný na portu 81. Pokud tedy zadáme ve webovém prohlížeči adresu http://server1.jirkasemrad.cz:81 objeví se nám přihlašovací okno, kde zadáme příslušné údaje, tj. jméno a heslo. (viz Obr. 6).

Obr. 6 - ISPConfig login

Zdroj: *vlastní*

[11] [XX]

Po úspěšném přihlášení se dostaneme do sekce pro správu a nastavení, a podle příslušných rolí a práv můžeme spravovat náš účet.

Obr. 7 - Administrátorské prostředí ISPConfig

Zdroj:*vlastní*

Administrátorské prostředí je podle hierarchie postaveno nejvýše a obsahuje základní nastavení serveru, správu účtů, DNS, FTP a dalších nastavení.

V následující tabulce jsou rozděleny práva jednotlivých účtů.

Tab. 6 - Jednotlivá práva v ISPConfigu

Administrator	Reseller	Customer	User
Měnit nastavení serveru	Vytvořit účet Customera a číst jeho statistiky	Číst webové data a statistiky	Měnit nastavení mailové schránky
Vytvořit účet Resellera a číst jeho statistiky	Vytvářet a administrovat webové stránky	Vytvářet a spravovat users účty a emailové schránky	
Vytvářet zálohu databáze ISPConfigu	Vytvářet DNS vstupy	Vytvářet a spravovat domény a subdomény	
Editovat DNS vstupy		Spravovat SSL certifikáty	
		Spravovat MySQL přístupová data	

Zdroj: *ISPConfig.org, 23.12.2009*

6.2.1.ISP Management

ISPConfig je rozdělen do několika poměrně přehledných sekcí. Začněme tedy tou první a tedy kartou Management. Jak celá sekce vypadá, je možné vidět v Příloha B. V této sekci nastavujeme základní nastavení serveru, např. jméno serveru, doménu, IP adresu, administrátorský email, list IP adres (v případě že máme více serverů využívající ke své správě ISPConfig), FTP a DNS server, a další základní nastavení. Také tato sekce slouží jako nástroj pro zálohu databáze, zjištění jejího stavu, její optimizaci a její opravu. Dále zde najdeme Update Manager, díky kterému udržujeme ISPConfig aktualizovaný. Pokud se na stránkách programu objeví nová verze, můžeme si ji volně stáhnout a pomocí Update Manageru ji nahrát aniž by došlo k výpadku serveru.

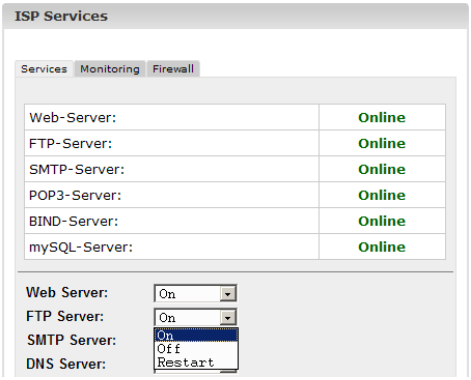
Pokud se podíváme blíže na nastavení serveru, tak v mém případě je následující:

Obr. 8 - ISP Server nastavení

Zdroj: *vlastní*

Jak již bylo napsáno výše, na Obr. 8 můžeme vidět současné nastavení serveru, tak jak je nakonfigurováno ve složce Settings. Další důležitou položkou je Status. Zde najdeme přehled informací o serveru (např. čas jak dlouho je server online, počet připojených uživatelů, vytíženost systému, atd.), informace o stavu paměti a CPU, a v neposlední řadě také stav jednotlivých služeb, které jsou detailně rozepsány v kartě Services (Obr. 9) s možností jejich správy.

Obr. 9 - Přehled služeb běžících na serveru



Zdroj: *vlastní*

Jak již bylo popsáno výše, tato tabulka nám přehledně ukazuje, které služby jsou v provozu a funkční. Při nastavování konkrétních služeb nám částečně pomůže ISPConfig, ale pro detailnější nastavení musíme sáhnout do konfiguračních souborů jednotlivých služeb a v bashi je nastavit. Tady ve složce Services můžeme služby, které běží na našem serveru zapnout, vypnout či restartovat.

V kartě Services také najdeme monitoring. Monitoring nám primárně slouží jako přehled o web serveru, ftp serveru a MySQL serveru. Ale dá se samozřejmě rozšířit i na další služby, které jsou ISPConfigem ovládány a monitorovány. Monitoring zaznamenává dění na serveru a v případě výpadku informuje administrátora v podobě emailu. Bohužel pokud dojde k selhání emailového serveru, je tato služba nedostupná. V následující tabulce je stručný přehled služeb a příslušných portů, na kterých běží.

Tab. 7 - Služby a jejich porty

Služba	Standardní port
FTP server (Proftpd)	21
SSH server	22
Emailový server (Postfix)	25
DNS server (BIND)	53
Webový server (Apache)	80
IMAP	143
SSL	443
Vzdálený přístup	3389

Zdroj:*vlastní*

6.2.2.ISP Manager

ISP Manager slouží ke správě účtu, webových stránek, hostingového plánu a složek. ISP Manager je řešen pomocí stromečku, abychom měli detailní přehled o všech položkách a uživatelích, které jsme vytvořili. Administrátor vidí veškerá master data, limity a přístupová data všech resellerů. Pohled resellera je omezen jeho právy. Při přidávání nového Resellera má administrátor právo na omezení některých položek, podle toho jak uzná za vhodné. Týká se to hlavně počtu webových stránek, diskového prostoru a dalších služeb. Reseller rovněž využívá ISP Manager pro administraci customers a webových stránek.

6.2.3.Ostatní položky a nastavení ISPConfigu

Mezi další položky rozhranní ISPConfigu patří DNS Manager sloužící k zadávání doménových jmen a adres pro webové stránky. IP adresy jsou rozdělovány podle umístění stránek na jednotlivých strojích (pokud jich máme více-větší hosting než jeden server).

Web-FTP je položka, která umožňuje pro tu danou stránku, resp. účet, ftp přístup a nahrání obsahu webové stránky.

ISP Invoice je „účetní kniha“. Zde se dají nastavit ceny pro domény, služby, webové stránky, tradic, emailové adresy, atd. Je zde přehled položek Customers a Resellers, jejich případné

fakturační údaje a položky, které mají uhradit. Vzhledem k tomu, že za webhosting se platí většinou paušálně, nemusí být ISP Invoice plně využit.

6.3. Webhostingové řešení pod lupou

Tato kapitola se věnuje testování a hodnocení webhostingové aplikace z pohledu bezpečnosti, dostupnosti a konektivity (rychlost odezvy, počet dotazů za vteřinu).

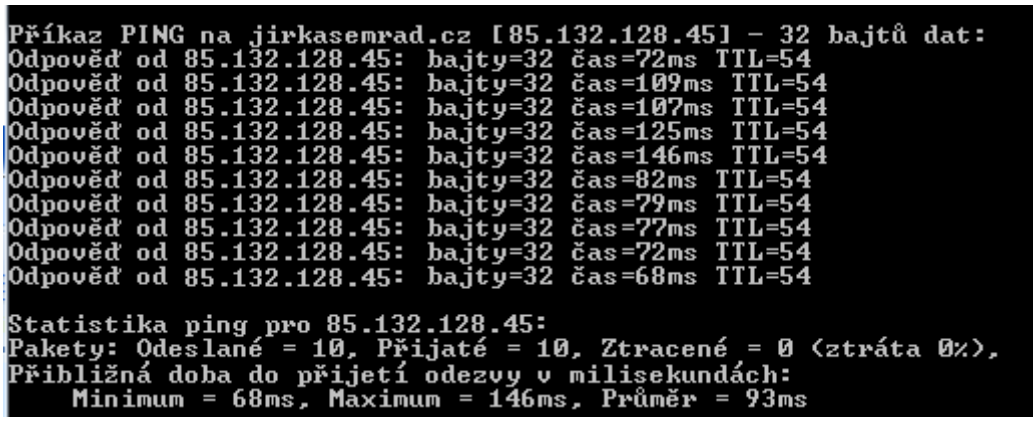
6.3.1.Konektivita

Server je umístěn pro testování v domácím prostředí, z čehož plyne, že jeho odezva dosahuje vyšších hodnot než odezva serverů, které jsou připojeny na extra rychlém, páteřním a optickém internetovém připojení. Některé komerční servery jsou připojeny rychlostí až 10 Gbps[12], což není absolutně možné v domácích podmínkách dosáhnout. Rychlost mého připojení se pohybuje cca. mezi 5-6Mbps. Rychlost odezvy záleží na počtu aktuálně připojených klientů, vytíženosti serveru v podobě počtu dotazů za sekundu, případně uploadu dat a dalších aktivit, které snižují rychlost připojení.

Test odezvy jsem provedl pomocí příkazu

ping jirkasemrad.cz -n 10

Obr. 10 - test rychlosti odezvy



Zdroj: *vlastní*

Další test jsem provedl pomocí webové stránky host-tracker.com, kde jsem testoval odezvu na můj server z různých zahraničních portálů. Výsledky testu jsou k vidění v následující tabulce.

[12] G2Server, připojení do NIX.CZ

Tab. 8 - Doba odezvy

Location	Ip	Time	Partner
Dallas, TX, US	85.132.128.45	(0 ms, 149 ms) 149 ms	Host-tracker.com
Dallas, TX, US	85.132.128.45	(0 ms, 147 ms) 147 ms	Arvixe.NET Hosting
Kiev, UA	85.132.128.45	(0 ms, 48 ms) 48 ms	HostBizUa
Moscow, RU	85.132.128.45	(0 ms, 59 ms) 59 ms	MosHoster.ru
Atlanta, GA, US	85.132.128.45	(0 ms, 118 ms) 118 ms	Valkira
Amsterdam, Netherlands	85.132.128.45	(0 ms, 25 ms) 25 ms	Seo ranking monitor
Zagreb, Croatia	85.132.128.45	(0 ms, 28 ms) 28 ms	Valkira
Melbourne, Victoria, AU	85.132.128.45	(0 ms, 357 ms) 357 ms	Apexhost.com

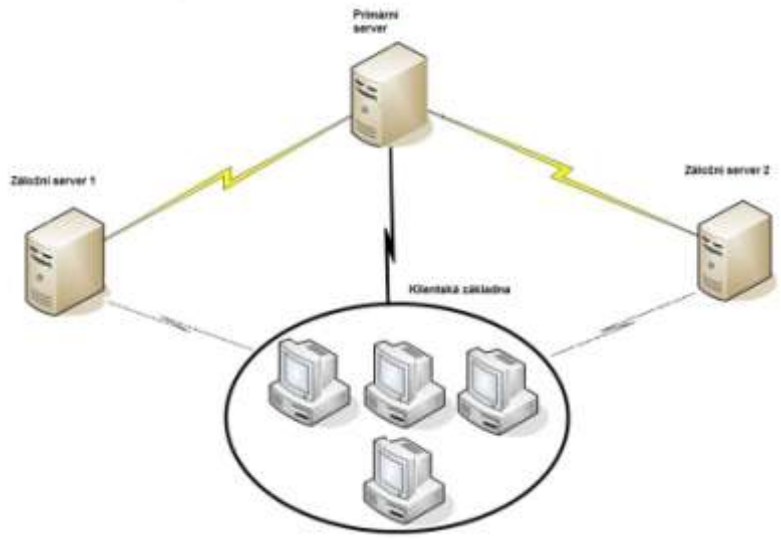
Zdroj: *host-tracker.com, vlastní*

Jak jsem již psal, doba odezvy je hlavně ovlivněna rychlostí internetového připojení a vzhledem k tomu, že server je nyní připojen k domácímu připojení cca 5-6Mbit jsou odezvy poměrně vysoké. V případě komerčního řešení, resp. využití pro mnohem širší účely hostingu by server musel být připojen k řádově 1-10Gbps jehož cena se pohybuje řádově v desítkách tisíc korun na rozdíl od domácí konektivity, která je dostupná do jednoho tisíce korun.

6.3.2. Bezpečnost

Kapitolu bezpečnost bych rozdělil do minimálně dvou podkategorií. Tou první by byla hardwarová bezpečnost a odolnost vůči okolním podmínkám. Jak už bylo naznačeno v kapitole 4.2, jedná se o zálohované napájení pomocí UPS, popř. diesel agregátem v případě dlouhodobějšího výpadku elektrické energie. Dalším prvkem ochrany může být připojení na dva nezávislé vysokonapěťové okruhy. Proti vnějšímu poškození může pomoct uzamykatelný a odolný rack. V místnosti se serverem by měla být umístěna klimatizace pro udržování vhodné teploty. V případě požáru inertní hasící plyn. Co se týká úložiště dat, tak nejlepším řešení pro jejich zálohování je duplicita serveru s tím, že jeden se bude nacházet např. v Praze a druhý např. v Brně. Pražský server jako hlavní a brněnský jako záložní, ale v případě výpadku pražského serveru ho může brněnský kdykoliv zastoupit neboť data jsou simultánně kopírována z pražského na brněnský (viz Obr.11). Pro testovací účely nebylo nutné zajišťovat tyto prvky, protože řešení je pouze krátkodobé. Ale ten kdo chce předejít ztrátě dat vinou poškození serveru či nějakých výpadků, měl by dodržet dané požadavky a instrukce.

Obr. 11 - záloha serveru



Zdroj: *vlastní*

Dalším bodem je softwarová bezpečnost. Jak už bylo naznačeno, jedním z prvků ochrany je dobře nakonfigurovaný firewall, který filtruje příchozí a odchozí spojení, ale má za úkol i vyhledávání možných útoků, protokolování anomálií, autentizaci a autorizaci uživatelů.

Pomocí společnosti Agerit s.r.o. a jejich testu bezpečnosti jsem nechal svůj firewall otestovat na případné nedostatky. Výsledky testu ukázaly velmi dobrý stav zabezpečení. Firewall je nakonfigurován, aby povolil komunikace pouze na portech 80 a 81, což jsou porty pro webový server a správu ISPConfigu, a dále port 3389 pro vzdálenou správu serveru.

Pro chycení a odhalení útočníka existuje v Linuxu několik metod. Rád bych jich pár zmínil. Jednou z nich je instalace aplikace honeypot resp. honeyd.

6.3.2.1. Honeyd

Honeyd vytváří fiktivní server, který je velmi slabý na zabezpečení a útočník se zaměřuje na něj. Na tomto serveru běží všechny služby, má otevřené porty a tudíž je velmi zranitelný. Účelem je odvést pozornost útočníka od reálných strojů a zároveň pomocí IDS (Intrusion Detection System – software pro odhalování průniku) zjistit, jakou taktiku útočník použil a přizpůsobit naší bezpečnostní politiku u reálných strojů.

Po instalaci vytvoříme a následně nakonfigurujeme virtuální stroje tzv. honeypot. Jejich vytvoření proběhne pomocí příkazu

arpd -i eth0 10.0.0.10-10.0.0.12 kde IP adresy jsou cesty k fiktivním strojům

Pomocí souboru *honeyd.conf* nakonfigurujeme vlastnosti jednotlivých strojů, např. pro 10.0.0.10

```
create winxp                                        #Vytvoří virtuální stroj
set winxp personality "Microsoft Windows XP Professional"    #Nastaví server aby se „tvářil“ jako Win XP
add winxp tcp port xxx open                         # Otevře daný tcp port (několikrát zopakujeme)
add winxp udp port xxx open                         # Otevře daný udp port (několikrát zopakujeme)
.
.
.
set winxp default tcp action block                  # Nedefinované tcp porty budou blokované
set winxp default udp action block                  # Nedefinované udp porty budou blokované
bind 10.0.0.10                                      # Přidělení stroji IP adresy – 10.0.0.10
```

Tím jsme nastavili první stroj, a můžeme stejným způsobem nastavit i další stroje. Navíc z některých strojů můžeme udělat třeba FTP server, či poštovní server nebo linuxový server pomocí přidání příkazů

```
create ftpsrv                                       # Vytvoří ftp server
set ftpsrv personality "Microsoft Windows XP Professional"    #Nastaví server aby se „tvářil“ jako Win XP
add ftpsrv tcp port 21 "sh ftp.sh"                  # Reakce na volání FTP serveru

create linsrv                                       # Vytvoří ftp server
set linsrv personality "Linux 2.4.17"               #Nastaví server aby se „tvářil“ jako Linux
add linsrv tcp port 25 "sh smtp.sh"                 # SMTP
add linsrv tcp port 110 "sh pop3.sh"                # POP3
```

Tím jsme dokončili konfiguraci našich virtuálních strojů a následujícím příkazem je můžeme spustit

honeyd -f honeyd.conf
10.0.0.10-10.0.0.12

Nyní jsme schopni tyto stroje pingnout a nástrojem nmap i získat přehled o jejich portech. Honeyd ale umí vytvořit mnohem více, např. virtuální router, simulovat zpoždění či ztrátovost.

6.3.2.2. IDS

IDS také slouží jako určitý druhý firewall. Klasický firewall může být překonán přes otevřené porty, a pokud se tak stane, je útočník často rozpoznán IDS pomocí analýzy paketů. IDS na základě signatur a umístění paketů zjišťuje bezpečnostní rizika. IDS také dekóduje jednotlivé pakety a vyhledává obecné známky zranitelnosti a bezpečnostní hrozby.

V případě, že se nám podařilo v některém logu (například SSH logy) zachytíme IP adresu útočníka, který se pokusil napadnout náš server, můžeme ho vystopovat. Logy najdeme umístěny */var/log/messages*. V tomto souboru můžeme vidět neúspěšné logy, v případě úspěchu jsou vidět v souboru *lastlog*. Po spuštění příkazu *last* můžeme vidět, kam se podařilo útočníkovy přihlásit. Útočník po sobě často zanechá stopu v podově IP adresy, kterou můžeme vypátrat. Jednoduchým příkazem

dig -x IP adresa

získáme výpis, kde v sekci answer můžeme vidět i doménu, odkud se útočník připojil, a zjistíme si kontakt na správce domény, a případně můžeme nějakým způsobem řešit potrestání útočníka, pokud způsobil škodu. V případě, že se doména neobjeví, použijeme příkaz

whois IP adresa

a můžeme získat poměrně obsáhle informace o majiteli domény či správce sítě. Zadal jsem výpis své vlastní IP adresy, a dostal jsem kompletní informace o svém providerovi včetně kontaktních údajů na konkrétní osobu. Takže kdybych někoho napadl, a on se obrátil na mého providera resp. na policii, snadno by mě vystopoval. Stačilo zanechat svojí IP adresu v logu.

6.3.2.3. Zabezpečení serveru Apache

Pro lepší zabezpečení webového serveru Apache je nezbytná pravidelná aktualizace všech jeho součástí. Dalším bodem je zakázat, aby Apache posílal informace o své verzi, verzi operačního systému na kterém běží či jaké moduly Apache spravuje. Vše můžeme zakázat v konfiguračním souboru *http.conf* přidáním příkazu

ServerSignatu Off
ServerTokens Prod

První příkaz zakazuje zobrazení verze Apache a OS, druhý příkaz zobrazí v http hlavičce pouze jméno serveru, tudíž Apache. Dalším možným způsobem, jak zabránit napadení serveru je modul, který byl napsán přímo pro Apache. Tento modul se nazývá mod_security.

Obsahuje několik druhů bezpečnostních prvků, např. filtrování, limit uploadu, validace URL, maskování identity, atd. Mezi další body zabezpečení může patřit, že soubory s nastavením serveru může měnit a číst pouze superuživatel root. Tyto práva se dají nastavit následujícími příkazy

chown -R root:root /usr/local/apache
chmod -R o-rwx /usr/local/apache

Jako obrana proti DoS útoku může sloužit omezení velkých požadavků (requestů). Například omezení na 1MB pro jeden soubor provedeme příkazem

LimitRequestBody 1048576

Apache také umožňuje, aby byl přístupný pouze z vybraných IP adres, popř. aby požadavky z určitých adres vůbec nepřijímal. Pro zabezpečení serveru Apache existuje mnoho řešení a variant, a vyjmenovat je a popsat všechny není snad ani možné a ani to není náplní této práce, proto jsem jich vybral jen několik.

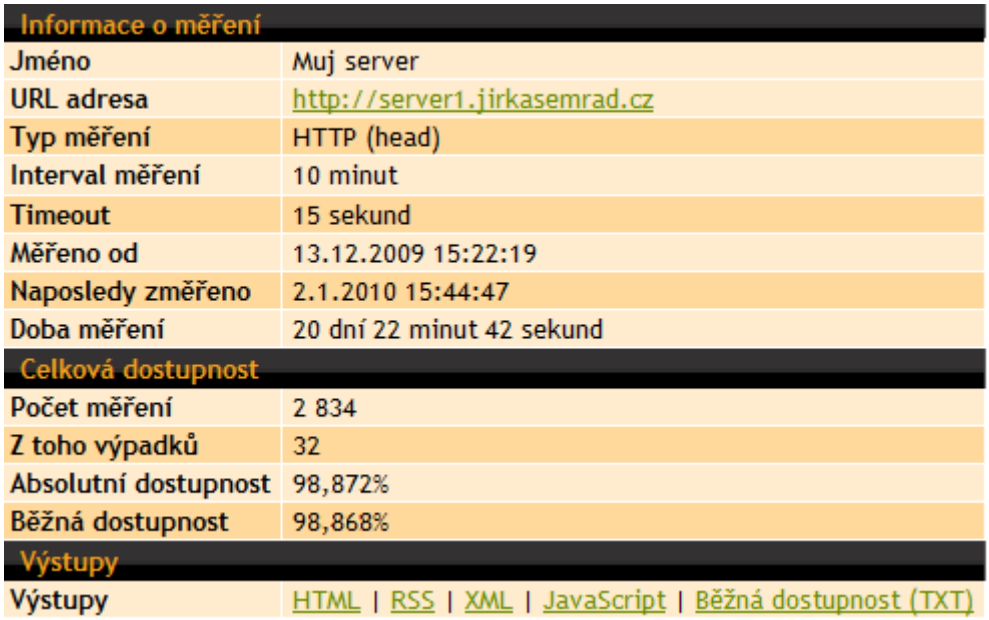
6.3.3. Dostupnost

Dostupnost je jedním z hlavních ukazatelů kvality webhostingu. Pokud chceme garantovat vysokou dostupnost služeb, musí být server dostupný max možný čas. To by znamenalo 100% měřeného času. V praxi toho není možné téměř dosáhnout. Musíme počítat s časem pro údržbu a aktualizaci serveru, výměnu porouchaných částí, upgrade hardware a atd. V praxi to znamená, že je server dostupný 99% za měsíc. V řeči čísel to znamená, že server nebyl dostupný cca 7 hodin měsíčně resp. 14,5 minuty denně. Zpravidla se údržba a podobné zásahy dějí v noci a drtivá většina uživatelů výpadek vůbec nepocítí. Výpadkům by se dalo zabránit duplicitou serverů, kdy bychom jeden server odstavili z důvodu opravy a celý webhosting by běžel na serveru druhém. Po dokončení oprav bychom provedli synchronizaci obou serverů a první server by se mohl stát opět nosným.

Svůj server jsem testoval pomocí webové stránky http://statistiky.monitoring-serveru.cz/ ,která bezplatně každých 10 minut odešle dotaz na dostupnost serveru. Server v té době byl online cca 20 dnů a bylo provedeno přes 2800 měření na dostupnost. Z tohoto počtu byl server 32x nedostupný. Celková dostupnost tedy byla cca 98,8%. Nedostupnost serveru mohla způsobit hlavně konektivita, neboť server je připojen na hifi, u které dochází k občasným výpadkům. Dalším faktorem je frekvence měření. Frekvence byla nastavena na 10 minut, což v praxi znamená, že výpadků mohlo být mnohem více. Pro přesnější výsledky bych musel

zaplatit určitý poplatek a pak by mohla být frekvence i 15s a výsledek by byl mnohem přesnější. Nicméně si myslím, že pro testovací účely tato má dostačující význam.

Obr. 12 - Dostupnost serveru



Informace o měření	
Jméno	Muj server
URL adresa	http://server1.jirkasemrad.cz
Typ měření	HTTP (head)
Interval měření	10 minut
Timeout	15 sekund
Měřeno od	13.12.2009 15:22:19
Naposledy změřeno	2.1.2010 15:44:47
Doba měření	20 dní 22 minut 42 sekund
Celková dostupnost	
Počet měření	2 834
Z toho výpadků	32
Absolutní dostupnost	98,872%
Běžná dostupnost	98,868%
Výstupy	
Výstupy	HTML | RSS | XML | JavaScript | Běžná dostupnost (TXT)

Zdroj:*vlastní*

7. Závěr

Při vypracovávání této práce jsem se dozvěděl mnoho nových informací a poznatků o jednotlivých částech webhostingové řešení. V první řadě určitě hodně informací o webových serverech, dále o operačním systému Linux a jeho možnostech, a v neposlední řadě jsem se přiučil mnoha věcem týkající se bezpečnosti počítačových sítí, jejích komponent a zabezpečení proti vnějšímu útoku.

V dnešní době existuje velké množství společností a firem zabývajících se webhostingem a jeho poskytováním. Některé z nich se zabývají touto problematikou ve velkém měřítku, tím že provozují desítky serverů, jiné společnosti se spokojí jen s několika servery. Od toho se také odvíjí jejich kvalita a cena poskytovaných služeb.

Mým cílem při vypracování této práce bylo navrhnout webhostingové řešení s ohledem na ekonomickou stránku, jinými slovy, pokusit se zrealizovat co nejefektivnější řešení za co nejnižší náklady. Proto jsem se rozhodl jít cestou softwaru s open-source licencí a zvolil jsem pro svoje řešení operační systém Linux, webový server Apache, ISPConfig neboli software pro správu webhostingu, a další prvky rovněž poskytované pod svobodnou licencí. Na druhou stranu jsem se rozhodl nešetřit na hardwaru a oslovil jsem např. společnost IBM, jednoho z významných dodavatelů serverů. Další položkou, na které bych určitě nešetřil, je konektivita mého serveru, protože ta patří společně s dostupností mezi základní pilíře spokojenosti zákazníka, resp. uživatele. Jak již jsem se zmínil, v případě, že bych chtěl snížit svoje náklady na hardware, mohu samozřejmě nakoupit levnější komponenty, ale u nich hrozí větší poruchovost. A v případě ztráty dat, která byla uložena na mých serverech, budu čelit velké nevoli mých zákazníků a v mnoha případech je mohu i ztratit.

Webhosting je služba, bez které se dnes neobejde téměř nikdo, ať už provozuje svou živnost pomocí Internetu, popř. využívající Internet pro propagaci své společnosti, firmy nebo sama sebe. Samozřejmě i další lidé, kteří by si chtěli jen přečíst jakýkoliv článek na Internetu se bez webhostingu neobejdou.

8. Seznam použité literatury

I. **AULDS, CH. 2000.** *Linux Administrace serveru Apache.* Praha : Grada, 2000. 563 s ISBN 80-247-0640-7.

II. **BANAN.CZ. 2009.** Firewall. *Banán.cz.* [Online] 2009. Dostupný z WWW : http://www2.banan.cz/cz/show/105.

III. **BRŮHA, L. 2008.** Audit a bezpečnostní analýzy IX. *Databázový svět.* [Online] 2008. [Cit. 09-04-09] Dostupný z WWW : http://www.dbsvet.cz/view.php?cisloclanku=2008120401.

IV. **BURNHAM, C. 2001.** *Web hosting.* The McGraw-Hill Companies, 2001. ISBN 00-721-3279-5.

V. **CAFOUREK, B. 2009.** *Správa Windows Serveru 2008.* Praha : Grada Publishing a.s, 2009. 288 s ISBN 80-247-2124-4.

VI. **CAMBRIDGE UNIVERSITY. 2007.** Exim Internet Mailer. [Online] 2007. [Cit. 09-03-22] Dostupný z WWW : http://www.exim.org/.

VII. **DENT, K. D. 2005.** *Postfix: Kompletní průvodce.* Praha : Grada Publishing a.s., 2005. 252 s ISBN: 8024710293

VIII. **HUCK, M. 1999.** *Microsoft Windows NT Server 4.0 versus UNIX. ,* Penguin.cz. [Online] 1999. [Cit. 09-03-25] Dostupný z WWW : http://www.penguin.cz/~had/unix-nt/.

IX. **JANÁK, M. 2009.** *Odpovědnost poskytovatelů služeb informační společnosti působících na Internetu.* IT právo. [Online] 2009. [Cit. 09-12-27] Dostupný z WWW : http://www.itpravo.cz/index.shtml?x=2149387.

X. **JELÍNEK, L. 2008.** *POP3 nebo IMAP?* Aiken Blog. [Online] 2008. [Cit. 09-03-20] Dostupný z WWW : http://www.aiken.cz/article/pop3-nebo-imap.

XI. **KIRCH, J. 1999.** Microsoft Windows NT Server 4.0 versus UNIX. [Online] 1999. [Cit. 09-03-20] http://www.penguin.cz/~had/unix-nt/.

XII. **KOUDELKA, P. 2003.** Historie operačních systémů. [Online] 2003. [Cit. 09-04-10] Dostupný z WWW : http://airborn.webz.cz/histos.html.

XIII. **KRČMÁŘ, P. 2008.** *Linux je na 70 % českých serverů, Apache na 88 %.,* Root.cz. [Online] 2008. [Cit. 09-04-10] Dostupný z WWW : http://www.root.cz/clanky/exkluzivne-linux-je-na-70-serveru-apache-na-88/.

XIV. **KRČMÁŘ, P. 2004.** *Linux tipy a triky pro bezpečnost.* Praha : Grada Publishing,a.s., 2004. 208 s ISBN 80-247-0812-4

XV. **KROPÁČKOVÁ, A. 2006.** *Bezpečnost elektronických dat a elektronické komunikace.* Zpravodaj ÚVT MU. [Online] 2006. [Cit. 09-11-21] Dostupný z WWW : http://www.ics.muni.cz/zpravodaj/articles/522.html.

XVI. **KURFIRST, M. 2006.** *Historie operačních systémů Windows, Unix, Mac OS a Linux.,* Můj Mac. [Online] 2006. [Cit. 09-04-11] Dostupný z WWW : http://www.mujmac.cz/art/polemiky/historie-operacnich-systemu-win-unix-macosx.html.

XVII. **MACEK, P. 2008.** Sendmail: pošťák, který nekouše. [Online] 2008. [Cit. 09-03-22] Dostupný z WWW : http://www.root.cz/clanky/sendmail-postak-ktery-nekouse/.

XVIII. **MACEK, R. 2001.** SUN PŘIJÍMÁ AGRESIVNÍ CENOVÁ OPATŘENÍ NA PODPORU PŘECHODU OD IIS K iPLANET. [Online] 2001. [Cit. 09-03-16] Dostupný z WWW : http://cz.sun.com/tiskove_zpravy/2001/10/iPlanet.html.

XIX. **MATEJKA, J. 2001.** Odpovědnost poskytovatelů web-hostingu za cizí obsah. [Online] 2001. [Cit. 09-12-14] Dostupný z WWW : http://www.lupa.cz/clanky/odpovednost-poskytovatelu-web-hostingu-za-cizi-obsah/.

XX. **MOUČKA, B. 2005.** *Vylaďte si svůj SpamAssassin*. Zpravodaj ÚVT MU. 2005, stránky 8-12. *ISSN 1212-0901*

XXI. **MYERS, J. 1996.** Post Office Protocol - Version 3. [Online] 1996. [Cit. 09-03-20] Dostupný z WWW : http://www.ietf.org/rfc/rfc1939.txt.

XXII. **POŠMURA, V. 2002.** *Apache Příručka správce WWW serveru.* Praha : Press Computer, 2002. 318 s, ISBN 80-7226-696-9

XXIII. **PŘIBYL, A. 2007.** *Proč používat Linux*. Kde získat Linux a jaký si vybrat. [Online] 2007. [Cit. 09-04-11] Dostupný z WWW : http://proc.linux.cz/kde-ziskat.html.

XXIV. **PUŽMANOVÁ, R. 2004.** *TCP/IP v kostce.* České Budějovice : Kopp, 2004. 607 s ISBN 80-7232-239-2

XXV. **ROSEBROCK, E., FILSON, E. 2004.** *Linux, Apache ,MySQL a PHP.* Praha : Sybex, Grada, 2004. 344 s, ISBN 80-247-1260-1

XXVI. **ROXEN, INTERNET SOFTWARE** [Online] 2009. [Cit. 09-03-19] Dostupný z WWW : http://www.roxen.com/products/.

XXVII. **SATRAPA, P. 1994 ,***Počítačové sítě*, prezentace TUL, 2007. Dostupný z WWW : http://www.kit.tul.cz/~satrapa/vyuka/site/prednaska01.pdf

XXVIII. **Satrapa, Pavel. 1997.** HTML v příkladech. *HyperText Transfer Protocol.* [Online] 1997. [Cit. 09-11-17] Dostupný z WWW : http://www.kit.tul.cz/~satrapa/docs/wwwprikl/html9.html.

XXIX. **SATRAPA, P., RANDUS, J. A. 1996.** *Linux - Internet server.* Praha : Neokortex, s.r.o., 1996. 413s, ISBN 80-902230-0-1

XXX. **SMEJKAL, V. 2002.** *Je Internet kriminogenní?* Praha : Vysoká škola ekonomická v Praze, [Online] 2002. [Cit. 09-10-22] Dostupný z WWW : http://www.rodiny.cz/f/Image/fotkyNCR/smejkal.doc

XXXI. **ŠINDELÁŘ, A. 2005.** MAC OS X je taky Linux. [Online] 2005. [Cit. 09-04-12] Dostupný z WWW : http://www.root.cz/clanky/mac-os-x-je-taky-unix-1-historie/

XXXII. **TOXEN, B. 2003.** *Bezpečnost v Linuxu.* Brno : Computer Press, 850 s., 2003. ISBN 80-7226-716-7

XXXIII. **VALÁŠEK, M. 2007.** Představení Internet Information Services (IIS) 7.0. [Online] 2007. [Cit. 09-03-20] Dostupný z WWW : http://www.aspnet.cz/Articles/159-predstaveni-internet-information-services-iis-7-0.aspx.

XXXIV. **VYCHODIL, V. 2005.** *Linux Příručka českého uživatele.* Brno : CP Books, a.s.,280s., 2005. ISBN 80-7226-333-1

XXXV. **ZAJÍC, P. 2005.** MySQL - pestrý svět databází. [Online] 2005. [Cit. 09-03-22] Dostupný z WWW: http://www.linuxsoft.cz/article.php?id_article=731.

XXXVI. **ZAJÍC, P. 2004.** PHP. *linuxsoft.cz.* [Online] 2004. [Cit. 09-11-14] Dostupný z WWW : http://www.linuxsoft.cz/article.php?id_article=171.

XXXVII. **ZEUS, TECHNOLOGY LTD. 2009.** Service Security and Network Reliability. [Online] 2009. [Cit. 09-03-19] Dostupný z WWW : http://www.zeus.com/products/zws/security.html.

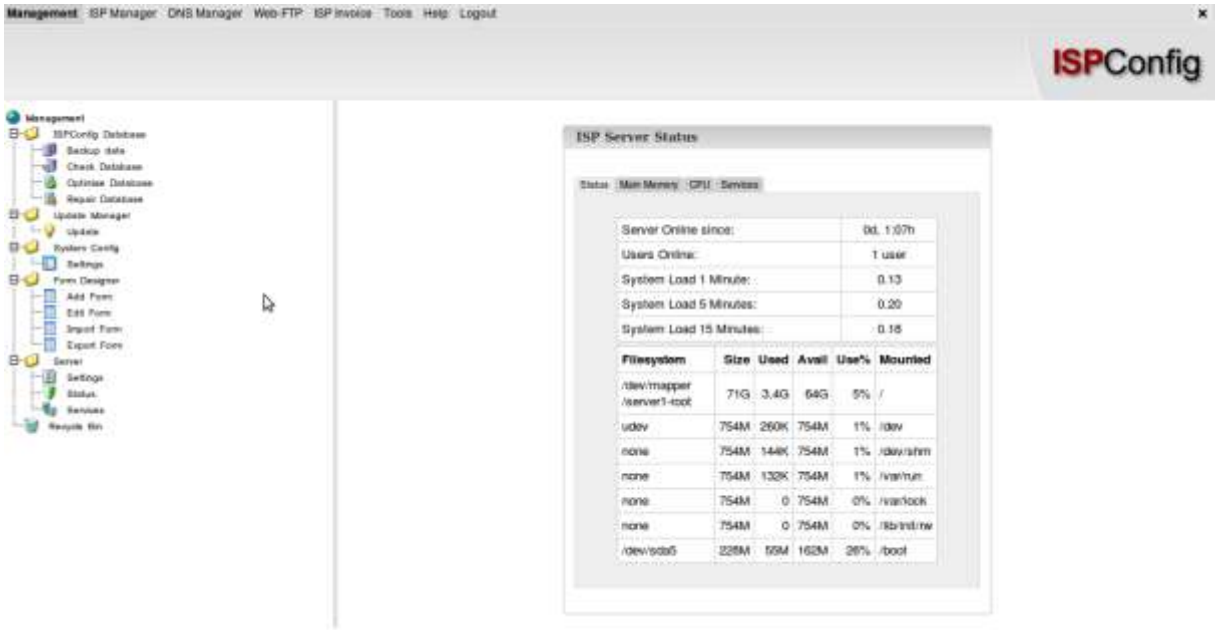
9. Seznam příloh

Příloha A – Nastavení Postfixu

Pro vyzkoušení funkčnosti SMTP a TLS jsem použil příkazy: *telnet localhost 25* a *ehlo localhost*

root@server1:/etc/postfix/ssl# telnet localhost 25
Trying ::1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 server1.jirkasemrad.cz ESMTP Postfix (Ubuntu)
ehlo localhost
250-server1.jirkasemrad.cz
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN

Příloha B – ISP Management



Příloha C - ISP Manager